DNA 6309P

THE ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY PROCEEDINGS OF THE FIFTH ANNUAL SYMPOSIUM, JUNE 11-12, 1980

Jennifer L. Gagnon and
Ann Ramey-Smith/Editors
Center for Consumer Product Technology
U.S. Department of Commerce
National Bureau of Standards
Washington, DC 20234

1 June 1981

Proceedings for 11-12 June 1980

DNA IACRO No. 80-829

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

THIS WORK WAS SPONSORED BY THE DEFENSE NUCLEAR AGENCY UNDER RDT&E RMSS CODE B310080465 B99QAXRA10107 H2590D. ADDITIONAL SPONSORS WERE THE LAW ENFORCEMENT STANDARDS LABORATORY AND THE CONSUMER SCIENCES DIVISION OF THE NATIONAL BUREAU OF STANDARDS, WASHINGTON, DC 20234.

Prepared for
Director
DEFENSE NUCLEAR AGENCY
Washington, DC 20305

DISPOSITION

Destroy this report when no longer needed. Do not return it to the originator.

DISCLAIMER

The findings in this report are not to be construed as an official Department of Defense position unless so specified by other official documentation.

WARNING

Information and data contained in this document are based on the papers available at the time of preparation. No attempt has been made to edit papers. The views expressed in them are those of their authors and should not be construed as representing the Defense Nuclear Agency. Correctness is the sole reponsibility of the authors.

TRADE NAMES

The use of trade names in this report does not constitute an official endorsement or approval of the use of such commercial hardware or software. The report may not be cited for purposes of advertisement.

COMPONENT PART NOTICE

THIS PAPER IS A COMPONENT PART OF THE FOLLOWING COMPILATION REPORT:

(TITLE): Proceedings of the Symposium on the Role of Behavioral Science in Physical Security (5th Annual) Held at Gaithersburg, Maryland, on June 11-12, 1980.

(SOURCE): National Bureau of Standards, Washington, DC.

TO ORDER THE COMPLETE COMPILATION REPORT USE AD-A138 882.

THE COMPONENT PART IS PROVIDED HERE TO ALLOW USERS ACCESS TO INDIVIDUALLY AUTHORED SECTIONS OF PROCEEDINGS, ANNALS, SYMPOSIA, ETC. HOWEVER, THE COMPONENT SHOULD BE CONSIDERED WITHIN THE CONTEXT OF THE OVERALL COMPILATION REPORT AND NOT AS A STAND-ALONE TECHNICAL REPORT.

THE FOLLOWING COMPONENT PART NUMBERS COMPRISE THE COMPILATION REPORT:

AD#:	TITLE:
P002 914	Security System Operational Recording and Analysis (SSOPRA).
P002 915	Computerized Site Security Moniter and Response System.
P002 916	Behavioral Model of Shipboard Physical Security.
P002 917	Some Human Factors Aspects of Military Entry Control Systems.
P002 918	Impact Resistance of Concrete.
P002 919	Area Coverage Intrusion Detection Systems Research.
P002 920	The Potential of Olfactory Reception for Ultratrace Chemical Analysis.
P002 921	Quaddafi Has One of Our Nukes or Some Things We Need to Know About Behavioral Science and Security.
P002 922	Human Factors, The Error of Omission.
P002 923	Vigilance Performance of Security Force Personnel.
P002 924	Threat Assessments "Horse Before the Cart".
P002 925	Psychological Deterrents to Nuclear Theft.
P002 926	The Utilization of Emerging Technologies in Physical Security Systems.
P002 927	Ergonomic Data Base for Physical Security.
P002 928	The Effects of Weather Sensitivity on Stressed Personnel.
P002 929	Facility Intrusion Detection System.
P002 930	Job Performance and Brain Asymmetry: Relevance for Physical Security Personnel.
P002 931	Instrumentation for Security Force Evaluation and Training.
P002 932	GUIDAR Alarm Assessment.
P002 933	Overview.

COMPONENT PART NOTICE (CON'T)

AD#: TITLE:

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER DNA 6309P	2. GOVT ACCESSION NO. AD-A138 882	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) THE ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY PROCEEDINGS OF THE FIFTH ANNUAL SYMPOSIUM, JUNE 11-12, 1980		5. TYPE OF REPORT & PERIOD COVERED Proceedings for 11-12 June 1980 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Jennifer L. Gagnon and Ann Ramey-Smith, Editors		8. CONTRACT OR GRANT NUMBER(s) DNA IACRO 80-829
9. PERFORMING ORGANIZATION NAME AND ADDRESS U.S. Department of Commerce National Bureau of Standards Washington, DC 20234		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS Subtask B99QAXRA101-07
11. CONTROLLING OFFICE NAME AND ADDRESS Director Defense Nuclear Agency Washington, DC 20305		12. REPORT DATE 1 June 1981 13. NUMBER OF PAGES 232
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A since UNCLASSIFIED

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

This work was sponsored by the Defense Nuclear Agency under RDT&E RMSS Code B310080465 B99QAXRA10107 H2590D. Additional sponsors were the Law Enforcement Standards Laboratory and the Consumer Sciences Division of the National Bureau of Standards,

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Behavioral Science
Human Factors
Intrusion Detection System
Performance
Security Barriers
Security System
Threat Analysis
Training
Vigilance

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

This document contains the proceedings of the Fifth Annual Symposium on the Role of Behavioral Science in Physical Security, held on June 11-12 1980. The symposium provided a forum for presentation and discussion of current behavioral science and related contributions to physical security. Attendees included government personnel and private consultants under contract to the Defense Nuclear Agency currently engaged in research related to military security.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

18. SUPPLEMENTARY NOTES (Continued)

Washington, DC 20234.

ACKNOWLEDGMENTS

The Fifth Annual Symposium on the Role of Behavioral Science in Physical Security was organized and developed by Mr. Marvin Beasley, Nuclear Surety Directorate of the Defense Nuclear Agency, with the joint sponsorship of the Law Enforcement Standards Laboratory (LESL) and the Consumer Sciences Division, both of the National Bureau of Standards. This document was physically prepared and reviewed by LESL, under the direction of Daniel E. Frank, Manager, Security Systems Program.

FOREWORD

The Defense Nuclear Agency (DNA) is engaged in a continuing effort to enhance the security of nuclear weapons storage. In this effort, it is receiving technical support from the National Bureau of Standards' Law Enforcement Standards Laboratory (LESL), whose overall program involves the application of science and technology to the problems of crime prevention, law enforcement and criminal justice.

LESL is presently assisting DNA's physical security program with support in the chemical science and the ballistic materials areas, among others. At the time that the Fifth Annual Symposium on the Role of Behavioral Science in Physical Security was held, LESL also provided support to DNA in behavioral science. This area of research was deleted from the scope of the LESL activity at the end of fiscal year 1980.

Among the tasks being performed by LESL for DNA are the preparation and publication of several series of technical reports on the results of its researches. This document is one such report. This report includes three papers authored by members of the National Bureau of Standards who, at the time of the symposium, were providing support to DNA in the area of behavioral science. In the future, DNA will continue to pursue behavioral science research through support from organizations other than LESL.

Technical comments and suggestions are invited from all interested parties. They may be addressed to the authors,* the Law Enforcement Standards Laboratory, National Bureau of Standards, Washington, DC 20234, or the Defense Nuclear Agency, Washington, DC 20305, Attn: SONS.

Lawrence K. Eliason, Chief
Law Enforcement Standards Laboratory

*Points of view or opinions expressed in this volume are those of the individuals to whom they are ascribed, and do not necessarily reflect the official positions of either the National Bureau of Standards or the Defense Nuclear Agency.

PREFACE

These proceedings are the result of a symposium, the fifth of a series, held on June 11-12, 1980, at the National Bureau of Standards, Gaithersburg, MD. The purpose of the symposium was to continue to define the contributions that behavioral science can make to the enhancement of all aspects of physical security systems.

The symposium was jointly sponsored by the Department of Defense Physical Security Equipment Action Group, the Defense Nuclear Agency, and the Law Enforcement Standards Laboratory and Consumer Science Division, Center for Consumer Product Technology, National Bureau of Standards (NBS).

Mr. Samuel Kramer, Associate Director for Program Coordination, welcomed the attendees on behalf of the Director of the National Bureau of Standards and introduced Lt. Col. Barton Rinehart, Chief of the Nuclear Security Division, of the Defense Nuclear Agency. Lt. Col. Cletus Kuhla, as Chairman of the Department of Defense Physical Security Equipment Action Group (PSEAG), extended his welcome to the attendees and expressed the PSEAG's interest in behavioral research. Dr. Stanley Warshaw, Director of the Center for Consumer Product Technology at NBS, welcomed the group on the second day of the meeting and described the National Bureau of Standards' technical support in the area of physical security.

The editors wish to acknowledge the cooperation of the staff of the Defense Nuclear Agency, particularly Mr. Marvin C. Beasley, LTC Barton Rinehart, and LTC Cletus Kuhla. Special appreciation is also extended to Mr. Joel J. Kramer, Center for Consumer Product Technology, NBS.

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

FORMAL PAPERS

SECURITY SYSTEM OPERATIONAL RECORDING AND ANALYSIS (SSOPRA)

Robert R. Mackie, Ph.D.
Human Factors Research, Inc.

Introduction

SSOPRA is a developmental project aimed at defining operationally relevant, quantitative measures of man-equipment effectiveness in security systems. An attempt will be made to develop such measures through on-line recording of the sensor inputs and communication network at an updated operational weapons storage site. The project is aimed at filling an information void concerning present strengths and weaknesses in actual security system operation. Because no objective measures of operational performance are presently available, system effectiveness is uncertain, and objective performance feedback to security guard personnel is lacking. This in turn can lead to lack of job satisfaction, problems in sustaining vigilance, and uncertainties in the assessment of training effectiveness.

If the recording and analysis techniques to be used with SSOPRA prove successful, a longer range objective will be to package the system in a convenient form for use by the security system personnel themselves. It is intended that the system be as general as possible and thus be applicable to all sites having upgraded system.

Personnel Functions in Security Systems

Figure 1 presents a generalized model of security system functions in which system personnel play more or less critical roles. It will be an objective of SSOPRA to obtain objective measures of security guard performance as it may relate to many of these subsystem functions. Security systems are, first and foremost, surveillance systems. In Figure 1, the functions related to surveillance include (4) Attention Selection, (5) Stimulus Reception and Processing, and (6) Detection (of some significant event). While these functions have to some extent been automated in the updated systems, man's role remains critical, not only for immediate visual assessment, but also for screening decisions that influence the probability of valid detections and the incidence of false alarms. The performance measures related to these functions may vary as a function of site characteristics, environmental conditions, routine traffic, and, when available, intelligence concerning possible adversary action.

(7) Feature analysis and (8) Threat Evaluation and Localization encompass the all-important functions of signal pattern interpretation and source localization. Whereas the surveillance function is likely to be heavily concentrated on a single individual (the tower guard), threat evaluation and localization will often involve the alarm response team (ART) as well. Since ART is under control of the tower guard, the command and control function (Executive Control in Figure 1) becomes involved at this point. SSOPRA will attempt to develop quantified operationally meaningful measures related to these aspects of system performance.

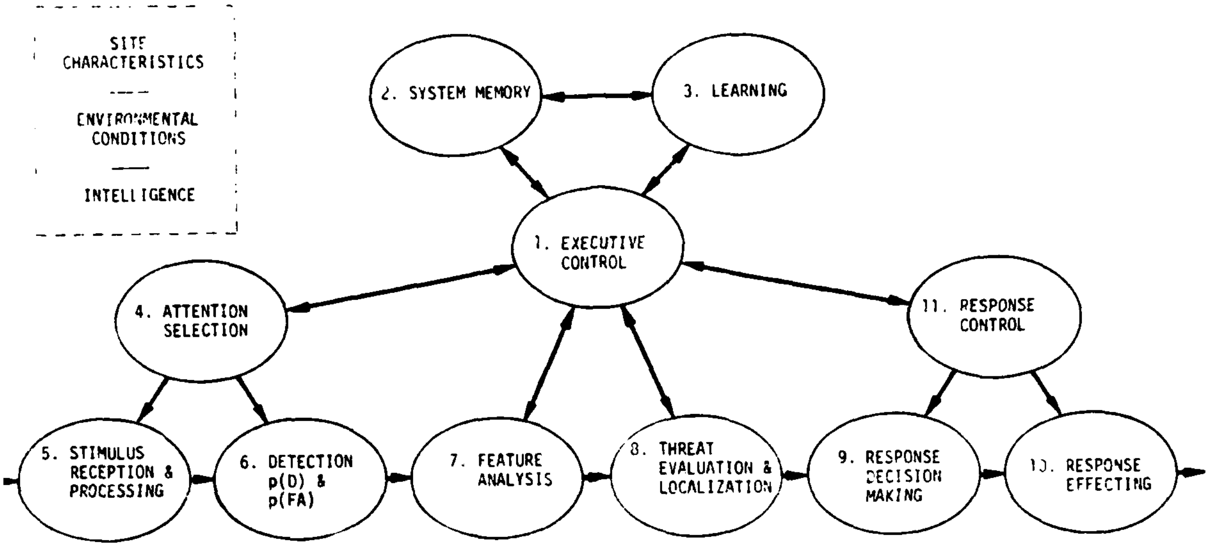


Figure 1. General functional model of behavioral elements in a security system.

The third major function of a security system involves the application of appropriate countermeasures to any genuine threat or intruder action. Thus it may involve the Fire Team as well as AR1. In Figure 1 these functions are identified as (9) Response Decision Making, (10) Response Effecting (threat neutralization) and (11) Response Control. Response Control refers to control at the scene of action as opposed to the more remote Executive Control exercised by the tower guard or by Central Security Control (CSC). SSOPRA will attempt to identify meaningful communication measures related to these functions though it will not directly address combat actions.

Two other "functions" are shown in Figure 1 which are not normally thought of as system functions. They are identified here as (2) System Memory and (3) Learning. Because the human element in any system learns to adapt to the routine demands and events of everyday operation, it can be expected that subjective probability estimates and memory for certain "expected" events will impact the probability of valid detection and the false alarm rate. For example, where there is a high "nuisance" alarm rate the human elements in a security system will "learn" that certain signal inputs are to be expected and can be safely ignored. There is clearly some risk in this type of adaptive response since knowledgeable adversaries might well take advantage of security guard expectations concerning the nature and significance of certain events. On the other hand, human screening of routine events, especially when they are large in number, is essential to manageable system operation. The alternative is to be in an almost continuous state of alarm, a condition that will not be tolerated for long by command. This is likely to be a problem area for physical security systems for some time to come, and we note it here because the SSOPRA measures may well reflect certain learned patterns of response that may or may not enhance system effectiveness.

Site Selection and Personnel

It is planned that an Air Force base with an upgraded system will be selected as the development site for SSOPRA. The performance measurement system will focus primarily on the SPCDS console operator, posted guards (if any), portal guards, roving patrols (ARTS) and the response force (fire team). At times we may also be concerned with the performance of back-up personnel in CSC.

The basic data that will be recorded includes all communications between these personnel on a round-the-clock basis, and the recording of all alarms resulting from any of several classes of initiating events. These include:

1. Visual reports
2. Perimeter alarms
3. Failure of a sensor system
4. Uncertain I.D.
5. Communication failure
6. Radio jamming
7. Fence alarms
8. Structure alarms
9. Possible intruder
10. Unannounced persons; vehicles, activities
11. Portal penetration
12. Evidence of guard duress

Video tape recordings will be made of the TV monitors and the map display whenever they are activated. All radio and telephone communications will be tape recorded through a voice actuated recording system. In addition, the output of the SPCDS printer will be collected as will copies of all official logs. The objective will be to record as fully as possible all initiating events and subsequent security team actions to those events in a manner that is totally noninterfering with actual operations.

It is anticipated that routine operational events will provide considerable data of interest. However, it is unlikely that the full security team will be exercised in all its responsibilities if we depend entirely on this "passive" technique. Thus it is anticipated that "active" procedures will also be employed. In these cases initiating events will be of the types commonly employed by evaluation teams. The number and variety of scenarios to be employed using active techniques remains to be determined.

Performance Measures

Since there is considerable methodological development involved in this project, it is not possible to specify in advance the detailed nature of the measures that will be obtainable. However, in general it is anticipated that measures of the following types may prove feasible:

1. Latency of initial response: sensor inputs/alarms
2. Interpretation of events: speed, correctness

3. Action decisions: latency, appropriateness

4. Delay times: arrival of patrols/fire team

5. Command and control: latency, appropriateness

All communications will be subjected to content analysis. A classification scheme will be developed for describing the function of each communication in terms of such criteria as (a) evaluating the situation; (b) reducing uncertainty; (c) command/control of remote personnel; (d) correction of error; and (e) superfluous information. A time-line analysis will also be performed of all communications and all identifiable actions taken.

Applications

In performing development work within the framework of actual operations there are always unforeseen limitations and difficulties that arise. Thus we cannot be confident that all of our development objectives will be met nor that all of the desired performance measures will be obtainable through the communications network. However, given even partial success, the contribution of SSOPRA to improved security system effectiveness should be considerable. The availability of objective data on man-equipment performance is, after all, fundamental to the assessment of how effective the system is now and in what areas improvement is most needed. Further, if we are successful, the SSOPRA measures should be applicable to:

1. the evaluation of new sensor equipment, or processors;

2. the identification of man-machine interface problems;

3. the evaluation of operational procedures and the impact of changes in procedure;

4. the diagnosis of deficiencies in training;

5. the evaluation of watch schedules and shift practices;

6. the validation of personnel selection procedures;

7. the refinement of performance standards;

8. the provision of objective performance feedback, and thus enhanced motivation and improved vigilance;

9. the avoidance of system suboptimization;

10. the refinement of security system performance models which urgently need meaningful measures of operationally relevant human response data.

DISCUSSION

QUESTION FROM THE FLOOR: You mentioned the possibility of black hat assaults as a test of the system. Will this be able to be conducted?

DR. MACKIE: We are advised by the Air Force personnel involved that they routinely do it themselves. They do have a standing board group whose responsibility is to conduct exercises rather routinely with respect to the activities black hats may engage in.

It is to be sure carefully guarded, and everybody early in the game knows it is an exercise. What we are counting on is an extension of what they themselves have been doing, and we do believe it will be possible.

What you cannot do as far as I can see at the present time is to actually initiate an event that will result in the call out of a fire team, for example, without the whole system knowing it is an exercise. That simply is beyond the scope of what we might be able to do.

We do think we will be able to initiate scenarios that will be meaningful. For example, even though it is an exercise, if that fire team is expected to be in place in forty seconds to take action against an intruder, we will know whether that team was called out, when it was called out, how long it took for that decision to be made, and how long it took them to get on station.

COMPUTERIZED SITE SECURITY MONITOR AND RESPONSE SYSTEM*

by

R. T. Moore
Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D. C. 20234

ABSTRACT. An integrated, state-of-the-art, computer-based system has been defined to enhance and improve the overall physical security of storage sites for nuclear weapons and materials. It would provide for the interconnection of a distributed network of computers with a survivable, fiber optics communications network. This distributed processing system would monitor and control the various physical security sub-systems on the site, including intrusion alarms and alarm assessment subsystems, access control equipments, deterrent systems. Sensors responsive to meteorological and environmental stimuli are provided to permit the use of correlation techniques to identify certain classes of nuisance alarms. The system is intended to provide timely, accurate and unambiguous information about the site security status or the progress of an attack or intrusion attempt and to provide local security forces with appropriate preprogrammed response initiatives. Changes in site security status and the resulting response actions are automatically reported up-channel to higher command levels and reserve forces are automatically called out in situations where there is any question of the ability of local guard forces to cope. The problem of maintaining system reliability and maintainability without compromising system integrity and security receives special consideration.

Introduction

The safeguarding of high value assets has always required the investment of substantial resources in terms of both labor and technology in order to provide an effective level of physical security. By effective, we mean that the protection it affords against the perceived threat must be commensurate with its cost. The evaluation of effectiveness, however, must be continuously reappraised in order to cope with changing threats such as the increasing numbers of fanatical terrorist organizations or the enhanced technical expertise of potential adversaries.

Background

In the past, asset protection has typically been provided through the use of strongly constructed storage facilities, and most importantly, guard forces. Human guards, although excellent in terms of flexibility, are notoriously poor when operating as sensors in a dull, routine environment. Because of this, electronic sensors have been increasingly replacing human sensors over the past few decades. These electronic sensors have had to be upgraded as

*Contribution of the National Bureau of Standards not subject to copyright. This work sponsored by the Defense Nuclear Agency under: Subtask Code B99QAXRB203 and Work Unit Code 01.

technology advanced in order to support the continuing effort to stay ahead of the ever increasing adversary sophistication. Later, different types of sensors were used in combinations in order to increase the likelihood of detecting an intruder and to make defeat of the alarm system more difficult. Communications technology has permitted large numbers of sensors to be monitored from a central location and features have been incorporated to help protect these communications links from tampering and to monitor their integrity. The development of digital computers provided the opportunity to support activities over and above the monitoring sensors. These could include the issuance of response instructions for specific alarm or emergency conditions as well as the maintenance of disciplined controls on a variety of activities such as alarm reporting, guard activities or the authorization of access. Large scale integrated circuits have permitted a dramatic reduction in the cost of computer hardware and digital communication and have made it possible to design reliable, affordable security systems in which these and other desirable features can be accommodated. The Computerized Site Security Monitor and Response System is such a design and is intended to address the special requirements of storage sites for nuclear weapons.

System Description

Overview

A typical nuclear weapons storage area contains one or more magazines and a site security control center that are enclosed by a perimeter fence delimiting the restricted area. Generally, there is both an outer and an inner perimeter fence with a clear area between them. Typically, one or more types of sensors are installed in the clear area between the fences to protect against any attempted intrusion. The perimeter is generally segmented so as to provide geographical localization of an alarm to facilitate response by guard forces.

The weapons storage magazines are equipped with various types of intrusion alarms, and these may be supplemented with forced entry deterrent systems that may be activated on command. These will release agents that will impact one or more of the five human senses of either the security personnel or the adversary or both. The desired impact on an adversary is to impair his acuity or his will or his ability to continue an attack. The desired impact on security personnel is to enhance their capability of detecting, recognizing, and deterring the adversary objectives.

Under the Computerized Site Security Monitor and Response System (CSSMRS) concept, all of the intrusion alarms and deterrent systems in each magazine are monitored and controlled by a microprocessor that is located within the magazine. In a similar fashion, the intrusion alarms and deterrents that are associated with two adjacent perimeter segments are also monitored and controlled by a microprocessor that is physically located in a small protected housing that is well inside the inner perimeter fence. These remote microprocessors are in essentially continuous communication with a highly reliable central computer complex using dual fiber optic data links. Site security status information is disseminated from the central computer complex to two, independent guard control stations associated with the site security control center, and also to higher command headquarters. Strategically located closed circuit television cameras provide a capability for immediate alarm assessment, and the use of pyroelectric vidicons operating in the 8 - 12 micrometer infrared wave length region eliminates the need for special camera lighting facilities. A block diagram of the general arrangement is shown in Figure 1.

Remote Microprocessor

Each of the remote microprocessors accepts signals from a group of sensors and communicates the status of those sensors to the central computer. It also has provisions for testing in order to verify the performance of those sensors, for controlling a closed circuit television camera and for testing or actuating forced entrance deterrent systems upon receipt of commands from the central computer complex. Normally, the remote microprocessor functions in a slave mode responding to inquiries and commands from the central computer. These are expected to occur at intervals of one tenth second or less. Any remote microprocessor that fails to receive a signal from the central processor for three tenths of a second will immediately enter an autonomous mode of operation. In this mode, it assumes control of its own forced entrance deterrent systems and will activate them on its own authority in the event predetermined combinations of its intrusion sensors become alarmed. This arrangement helps prevent compromise of the system as a result of an adversary disabling either the central computer complex or the fiber optic data link loops.

When communication is restored between any remote microprocessor that is in the autonomous mode and the central computer, thatremote microprocessor automatically returns to the normal mode of operation.

Site Security Control Center

The site security control center includes the central computer complex and two independent guard control stations together with the necessary communications, control, display and emergency power facilities.

The central computer complex employs three identical processors that are operated in synchronism or "lock step" from a common (but redundant) clock. The data busses of the three central processors are compared to each other each computer cycle. A majority vote is taken, and when two out of three are in agreement the data is accepted as valid and acted upon. Any single computer whose output differs from the other two is immediately identified and is directed into a resynchronization routine in which its random access memory is reloaded from one of the "good" processors. This procedure is quite effective in correcting "soft" failures such as those caused by alpha particles or other similar non-crippling transient events. If no two computers agree, an operational problem exists that cannot be corrected automatically. A fourth processor is maintained as a spare to serve as an immediate replacement to correct any "hard" failure that may occur in one of the processors.

As an experiment, three microcomputers have been operated in our laboratory continuously for nearly a year in our triply redundant mode described above. During this period, there were more than fifty thousand successful resynchronizations, many resulting from deliberately induced transients. There were five outages. Two of these resulted from loss of power during thunderstorms since no emergency power supply was provided. Three of the outages were caused by component failures. Interestingly, during the week prior to one of the component failures, there were more than twenty thousand successful resynchronizations. It would appear that this component was causing a high rate of error occurrence as a precursor to its outright failure! In an operational environment the failing processor would have been identified and replaced before its complete demise.

On Site Communication

Communication between the central computer complex and the remote microprocessors located in magazines or perimeter stations is handled by "front end" communications microprocessors, each of which is capable of handling up to 24 remote stations. These are connected in a configuration that has been named "CROSSFIRE". It is a double loop in which the traffic flows in two independent but parallel rings. On one ring the data flows in a clockwise direction, and on the other ring, the same data flows in a counterclockwise direction. This data is identical in both content and timing at the transmitting station which may be either at the central station or a remote station. Data received at the central station is not repeated, while data received over each loop at each remote unit is immediately repeated and forwarded to the next station on each of the loops. Transmissions are in "frames" using the American National Standards Institute, X3.66 - 1979, Advanced Digital Data Communications Control Procedures. Transmissions over the fiber optic loops are at a speed of 56,000 bits per second and a continuous flow of traffic is maintained by polling each station in sequence .

When a frame is received at the addressed remote station, it arrives over the clockwise and counterclockwise loops at slightly different times. Upon arrival via each (or either) loop, the frame check sequence used for error control is computed. If it is correct, the frame is accepted for further processing. In addition, the frames from both the clockwise and counterclockwise loops are stored for a period of time no longer than required to insure the arrival of both under normal conditions, and are then compared, bit for bit. The remote station reacts to the frame in a manner that depends upon both the results of the frame check sequence test and the comparison of frame contents. If the check sequence is correct and the frame contents agree, operation is normal. The remote station acknowledges the frame and executes any command that it contained. If only one check sequence was correct, the addressed remote station must report the loop on which it did not receive the frame or upon which the check sequence was incorrect, and must execute any command contained in the frame with the correct check sequence. If the check sequence.is incorrect in the frame received over both loops, the frames are rejected and their contents ignored. If both frames have correct check sequences but their contents do not agree, this is an indication of a sophisticated attempt at spoofing, (or a very rare failure of the frame check sequence) and again the frames are rejected and their contents are ignored. If either of the latter conditions persist, the remote station enters the autonomous mode of operation.

Each of the up to 24 remote stations on a CROSSFIRE loop is polled every 0.1 second. Using the above described procedures, immunity is provided from any cutting, jamming or spoofing attack made at a single location on the dual loops. Further, through analysis of the sequence of responses from the remote stations, the site of any such attack can be localized within the time required for a single poll cycle.

Guard Control Stations

The two independent guard control stations provide the principal interface between the system and the site security personnel. One of the guard control stations is designated as the primary, and the other station, typically located in a surveillance tower, is designated a secondary station and serves as a backup to the primary. All controls, indicators and displays are duplicated in the two stations, and the guard at each location has the same capability to interact with the system.

Only one station and one operator is actually needed to operate and control the system. The second station has been added to increase the reliability of the system, to provide an extra monitor of operations, and to extend the two-man rule to station activities. It also increases the effectiveness and capability of the system during times of unusually high activity by permitting taks to overflow to the second station. It reduces the vulnerability in the event of an attack and loss of one of the stations.

System components that are available to the guards at each station include a digital display of alphanumeric data, four closed circuit television monitors, and a group of functional switches and controls. There is also communications equipment, automatic data logging equipment and a variety of audible and visible alarms and indicators. Every effort has been made to provide an arrangement for these controls and displays that will minimize the skill and training requirements of the station operators. For example, when an alarm condition occurs, audible and visible signals direct the guard to acknowledge the alarm, and the closed circuit television display of the appropriate area is automatically presented on one of the monitors. If the guard at the primary guard control station does not acknowledge the alarm condition within a few seconds, the guard at the secondary station is also specially warned, and if the acknowledgment is still not forthcoming, automatic messages are transmitted to call out reserve or augmentation forces as a precaution against the site being overrun with adversaries. When a guard acknowledges an alarm, audible warnings are silenced, flashing lights converted to steady state, and full details regarding the alarm and recommended response actions are presented on the CRT digital display unit. In addition, the same information is announced to him, audibly, by a speech synthesis system. The guard does not even have to have reading or typing skills in order to operate the system. Controls are functional, and where responses are required by system design, flashing lights indicate acceptable candidates for selection.

When several alarms occur within a short period of time, each must be acknowledged within the preestablished time interval. They are queued, and can be recalled at will be either or both of the guards for their assessment and disposition. A logging printer and an audio recorder provide records of all significant events associated with all alarms, and the logging printer also automatically records information significant to sensor tests, magazine accesses, maintenance actions, guard duty status and other administrative details.

Electronic Lock

The CSSMRS concept provides an opportunity for increased security in connection with the control of authorized personnel to access exclusion areas such as weapons magazines. This is realized through the use of an electronic lock as a replacement for one of the two key-operated mechanical locks that are currently employed in many situations.

The electronic lock is released by the matching of two numbers. The matching must occur within a limited time after access has been authorized, and only a single trial match is permitted. At the time that access to a magazine is authorized, the central processor generates a random number. This random number is stored in the computer memory and is also loaded into a portable electronic "key" which is given to the personnel that are authorized to make the access. When these personnel arrive at the designated magazine, they telephone the guard control center and advise that they are ready to make entry. The guard on duty signals the central processor of this readiness, and the random number stored in the computer memory is then transmitted to the remote microprocessor at the proper magazine. Upon receipt, this number is transferred to the buffers of the electronic lock which is located within the structure, and the lock is enabled for a one minute period of time. Successful matching of the random numbers in the lock with those carried in the key, after the letter has been plugged into an appropriate receptacle on the exterior of the magazine, causes an electrically powered solenoid to withdraw a bolt from its strike in the door sill. Only a single comparison is permitted within this one minute time interval. If the match of random numbers occurs, and the door is released, the fact of the release is reported to the guard control station. If a trial is made and the match does not occur, the enable period is terminated and an alarm condition is reported at the guard control station. An alarm condition is also reported if a match is attempted when the acceptance time is not enabled.

As a further precaution, the random number that is loaded into the portable battery powered key may be erased after a preset period of time. This interval is normally set to be only a few minutes greater than the travel time from the guard control station to the designated magazine. The combination of limited effective key lifetime and limited lock match acceptance time make it unlikely that a defecting guard could provide any advantage to an accomplice by throwing a key to him over the fences.

Manual Override

In this system, extremely high reliability has been a goal that is approached through the use of redundant components, backup sources of power and fail safe modes of operation. The latter, particularly when considered in association with forced entrance deterrent systems, require that special attention be given to the problems involved in performing corrective maintenance. A remote microprocessor, upon losing communications with the central computer complex, enters an autonomous mode of operation where it may actuate its deterrent systems if certain intrusion detection sensors become alarmed - as they might by the opening of a magazine to permit the authorized access of a maintenance technician. The problem is one of disarming or disabling the deterrents systems under such circumstances in a foolproof and reliable manner that does not also compromise security when the system is functioning in a normal manner.

The approach that has been adopted is the use of a mechanical, manually operated override device that guarantees the production of a high intensity audible alarm followed by a several minute waiting period before the deterrents are rendered safe and the door to the magazine can be opened. This override device is driven by a crank that is inserted from the exterior of the magazine and manually rotated. The speed of rotation is controlled by a governor mechanism that is arranged to disconnect the drive whenever the speed of rotation is excessive. This prevents using a motor drive to shorten the delay period. Operation of the crank advances a yoke on a lead screw. The initial motion of this yoke activates a high intensity horn that is powered by a tank of compressed gas such as dry nitrogen. The horn blast is directed out the ventilation louvres of the magazine door and is of sufficient intensity to be easily heard by all guard forces on the site. Further operation of the crank and motion of the yoke that it is driving has no effect for several minutes. At the expiration of the delay period, which may have involved several hundred revolutions of the crank, a cable withdraws the bolt of the solenoid normally used by the electronic lock and at this time the electrical actuation circuits to the deterrent systems are disabled. The resulting safe condition is mechanically signalled to the maintenance technician, who may now safely open the door and enter the magazine.

Conclusions

In this brief description of the Computerized Site Security Monitor and Response System it has only been possible to present some of the highlights of the design which has been described more fully in the references. In a complex system such as this, it is difficult to overstate the importance of human factors in the arrangement and configuration of the operating controls with which the guards must interact. Much effort has been devoted to making these simple to understand and easy to use so as to minimize guard training and skill requirements. Further refinements and improvements are expected to be tested under laboratory conditions and incorporated in a prototype system that will be subjected to field test and evaluation.

References

1. R. T. Moore, et al, "Computerized Site Security Monitor and Response System," NBSIR 77-1262, National Bureau of Standards, June 1, 1977, NTIS PB 269 346.

2. R. T. Moore, et al, "Phase II Final Report Computerized Site Security Monitor and Response System," NBSIR 79-1725, National Bureau of Standards, March 1979, NTIS PB 294343.

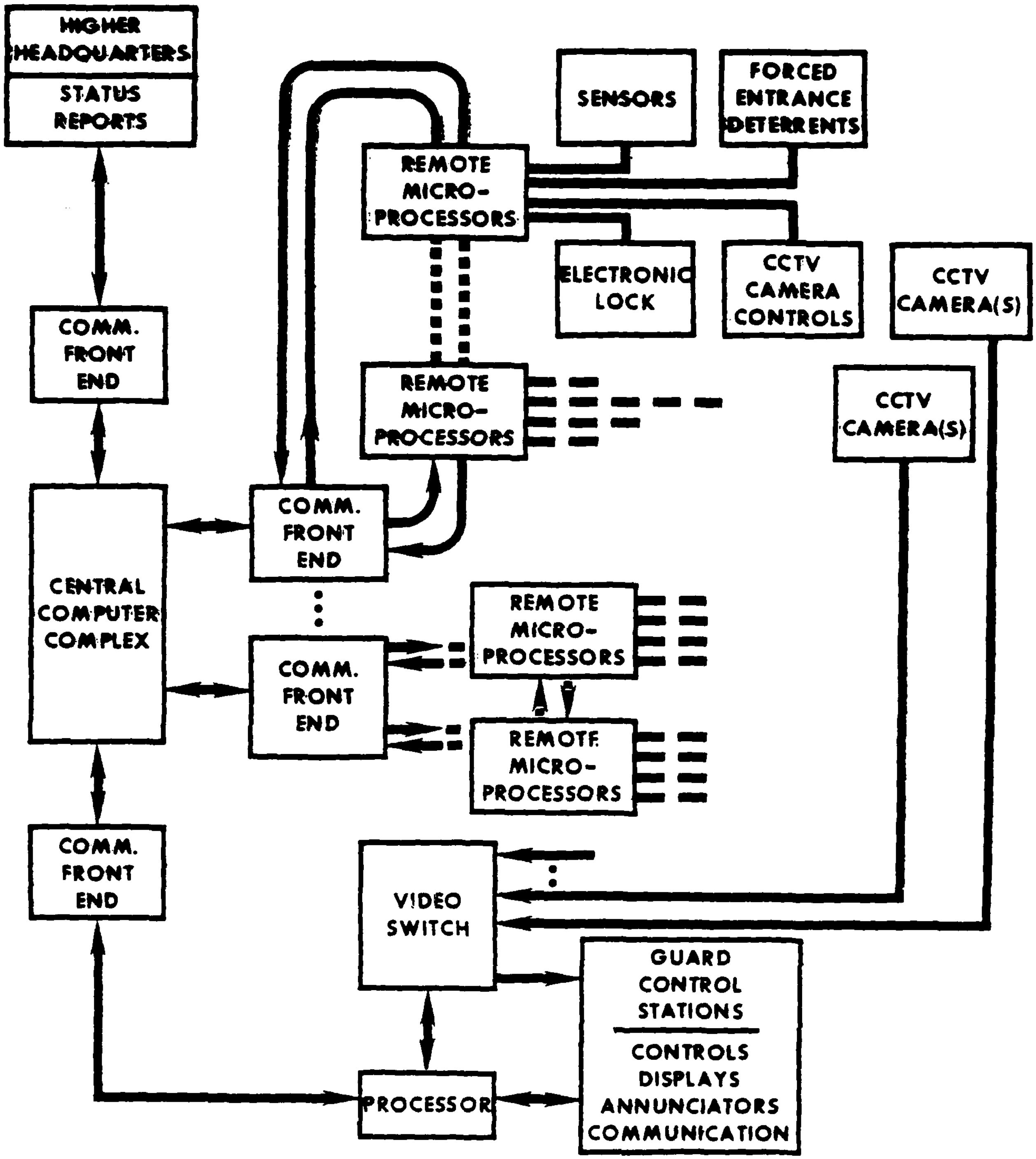


Figure 1. Simplified Block Diagram of the Computerized Site Security Monitor and Response System

DISCUSSION

COMMENT FROM THE FLOOR: This is more an observation than a question. Your comments about improved signal processing and reduction of nuisance alarms was of particular interest to me because it seems to me we face a design dilemma in that respect as long as the human is going to be part of the system. The dilemma is that nuisance alarms from the standpoint of maintaining human alertness and a sense of usefulness in a system are not all nuisance.

Nuisance alarms serve a significant function; virtually all vigilance theories would suggest that people who have to process a certain amount of input information are much more able to maintain a desired level of performance than people who are waiting endlessly for something to happen that is just so improbable that they face every watch period without any expectation that anything is going to happen at all.

In the upgraded sites, there has been a change in the roles of the area response team, for example, since the installation of the TV cameras. What happens is the tower guard processes virtually all alarms, nuisance or otherwise, and most of them are nuisance alarms or false alarms. This processing does not even filter down to the area response team which is on guard in a motorized vehicle at all times.

The result is the amount of time the response teams are asked to investigate something has been dramatically reduced, at least at this one site we have investigated. The prediction is that their effectiveness would tend to decrease.

I see this as a design dilemma in not just security systems but in all systems. As we increase the level of automation, we reduce the degree of human involvement in the processing of all information. Yet he is plugged in somewhere at a point where his ability to respond and to retain all of his necessary skills and so forth are really critical.

MR. MOORE: I appreciate the dilemma. One of the standard techniques for defeating the system is to throw a rock against the fence and create an alarm. A guard comes running out and there is nothing there. You do this four or five times. When he finally does not run out, that is when you go over the fence.

I do not know the answer either, but it is a very real problem.

BEHAVIORAL MODEL OF SHIPBOARD PHYSICAL SECURITY

Larry Ewing

Mission Research Corporation
P.O. Drawer 719
Santa Barbara, CA 93102

Mission Research Corporation under contract to Navy Personnel Research and Development Center (N00123-79-C-1446) is just completing the first phase of a three phase effort to develop a model of human behavior for ship security personnel and adversaries in scenarios that threaten nuclear weapon security. The model that will be developed is to be incorporated, either directly or by further simulation, into a larger model of the entire security system of a Navy ship.

Inasmuch as security systems of the present and near term are man intensive, and our particular focus for the Navy is shipboard security, principally nuclear weapon security, a model of a security system must also model the human element of the system. The human element is one of three major elements of a security system. Physical layout of the facility, barriers, and devices for delaying and deterring intruders is one element of the system. Sensors and their associated data processing systems that are designed to detect, to locate, to track, and to assess potential threats form the second system element. Security forces with their supporting equipment aids, weapons, formalized operating procedures, command structure, and communication/ control for the interdiction, engagement, and capture of intruders are the third system element.

In addition to various threats, the security system must contend with exogenous variables. These variables range from physical variables of weather and illumination, to stochastic events and neutral personnel. Physical variables and stochastic events are self-explanatory, but what, precisely, is meant by neutral personnel? In our model, a neutral human is neither a "friend" nor a "foe." By a friend we mean someone who is on the same team (security or intruder) and who can be counted on for help. By a foe, we mean someone who is on the opposite team and who represents a threat. These are our operational definitions of friend, foe, and neutral. Statements such as these may appear to be banal aphorisms that add nothing to what is known, but be assured such is not the case; they form the necessary foundation upon which a simulation can be built. For the security force, examples of neutral personnel are a visiting civilian or a fellow seaman who is not on the security team.

To analyze shipboard security, we generated seven scenarios that were chosen to cover a broad spectrum of threats: terrorists, activists, criminals, insiders, and pranksters. Following the reductionist philosophy of modeling, the scenarios were dissected to expose the human functions and to explore their interrelationships. Some functions take the form of solo actions, while other functions require the simultaneous interaction of two or more individuals. As the scenario for an attack against a ship evolves, personnel performance is degraded by fatigue and workload increase. This appears as an increased time to achieve a given probability of success or a lower probability of success in a given time. Human performance, the human element in the system, strongly affects scenario outcome.

Our objective in this work is to synthesize the previously identified system elements into a computer simulation of the system, focusing on the human element. The physical elements of a security system, exogenous variables that provide the environment, and personnel performance models that depict the functioning of security force, threat force, and neutral individuals are brought together in a scenario drama. The computer simulation is based on the planned attack scenarios and the standard operating procedures designed to thrwart attacks, so that it will model scenario evolution. One program run should be regarded as a realization of possible scenario outcomes drawn from an ensemble of such outcomes. Statistical results will be generated by "Monte Carlo" repetition of a scenario. More than the simple success or failure of the security system is of interest. The time history of the evolving scenario, personnel interactions and the transmission of significant information, man/machine interactions evaluated to determine the enhancement to security from automated system components, individual perception and response to threats, and evaluation of alternative standard operating procedures (SOPs) can be examined and tested as the model is used to probe for system weaknesses.

As part of the analysis of the seven candidate scenarios, we identified the human functions shown in Table 1. This table is not intended to be exhaustive, but rather indicative of the tyes of human activity that the behavior/performance model will have to simulate. Certainly, all scenarios do not need all of the listed functions, and it is relatively easy to invent a scenario that would require adding to the list. A large number of interesting scenarios and variations can be examined by providing a reasonably large subset of these functions. The list in Table 1 will lead to a program design that will provide for simple incorporation of similar function models, as they are required.

Input to the model for each individual in the scenario will be values we refer to as long-term variables. Although these quantities can change with time, their rate of change is slow when compared to the period over which a scenario will occur. Thus, for an individual in a scenario, they are fixed parameters. Attitude and dedication are subjective estimates and will be used largely to shortcut the formation of an individual's utility matrices. Input for attitude (motivation) and dedication will be quantized in two or three levels. Adaptation time constants will be input to model the dynamic response of eyesight and hearing to large signals. Physical condition and acclimation affect fatigue rate (fatigue is one of the dynamic variables in the model). These models will also be quantized in program input. Physical skills probably can be input as a level of proficiency; however, special skills may have aspects of strength, endurance, dexterity, coordination, and specialized knowledge. As a scenario progresses,

Table 1. Human functions in security scenarios.

	Group		
Function	Security team	Intruders	Neutrals
Administrate	X	X	
Liason	X	X	
Patrol	X	X	
Communicate			
send one-way	X	X	
rec. one-way	X	X	X
send two-way	X	X	X
rec. two-way	X	X	X
Move[a]	X	X	X
Hide	X	X	X
Wait	X	X	X
Capture	X	X	
Be captured	X	X	X
Escort	X	X	
Be escorted	X	X	X
Physical search	X	X	
Start battle[b]	X	X	
Take cover	X	X	X
Entry control	X		
Respond	X		
Monitor	X		
Challenge	X		
Investigate	X		
Neutralize		X	
Tamper		X	
Penetrate		X	
Steal		X	
Damage		X	
Arm		X	
Launch		X	
Special moves[c]		X	

Notes: [a] Common means of movement are creeping, walking, running, and climbing a ladder.

[b] MRC is not tasked to develop an engagement model, so the simulation can end with a commitment to fight.

[c] Special moves include swimming, rope climbing, rappeling, and riding a vehicle.

the dynamic variables could affect these dimensions in separate ways. So, in addition to proficiency level, each physical skill may have to be described as well in terms of other dimensions.

The model of human behavior we envision is not deterministic or mechanistic in its choice of response to a presented stimulus. We are not modeling a termite mound or a hive of bees. Decisions made by a human in our model will be based on his perception of his current situation and his knowledge of what has happened. Perceptions and prior knowledge can be inaccurate and incomplete. In the dynamics of a scenario, a decision must be made within a time window; if it is not, it has the same effect as having decided to wait, to gather more information, or simply to postpone the decision.

We view this cognitive decision making as a key element in the model. Model input in cognitive skill will include initial knowledge: operating procedures for the security force, scenario plan for the intruders, and any other prior knowledge that may be required to begin the simulation. Short-term memory will be modeled as the probability of recall with an exponential decay in which the decay is a function of both a time constant and the number of intervening events (stimuli). Long-term memory will be modeled as the storage and recall of facts from short-term memory being probabilistically dependent on the number of related facts in both memories. For example, an individual in the model may require three related facts in memory to reach a 0.5 probability of storing the fourth fact.

Evidence for the subjective truth of a concept, given relevant information, will be modeled as a Bayesian evidence function, which is defined as the logarithm of the ratio of the probability of truth to probability of falsity of the concept given known information. Experimental evidence indicates that such a model of human evidence weighting can be improved by discounting, to a degree, information that is drawn from memory in contrast to that which has just been experienced. This effect is known as base rate fallacy. Two threshold values will also appear in the use-of-evidence model. One threshold is the "preponderance of evidence" threshold. When the (subjective) probability of the truth of an hypothesis is above this threshold, it is always taken to be "true." The other threshold is the "marginal evidence threshold" which allows the modeled human to evaluate evidence with only a crude approximation to arithmetic accuracy. Only a computer and Mr. Spock of "Star Trek" evaluate probabilities to four or five decimal places. A human in the model will not be able to distinguish among alternative hypotheses when their probable truth is sufficiently close: when the difference in evidence functions is less than the second threshold. For hypotheses whose probabilities fall between these thresholds, the human accepts the "probable truth" of the greatest alternative. The truth of an hypothesis, for a modeled human, can then range from certainty to probably true, to ambiguous, to probably false, to clearly false. A similar use of thresholds applies to the decision model.

Decisions will be modeled as a risk analysis using the subjective utility of an outcome (given the information and action required) and the probability of that utility (given the perceived state of the world). If one utility-probability product is not a clear winner above an alternative distinguishing threshold, say 90 percent of the greatest value, the alternative set that appears similar could be normalized and a random draw used to decide--flip a coin. Or knowing the ambiguity of the situation, and given time to do so, the individual might choose to postpone the decision. The risk analysis decision model will not examine a tree of alternative branches; it will model only a single step look-ahead reaction-mode decision. We are not attempting to model strategy formulation in humans. All strategy is assumed to be embedded in the SOPs and attack scenario plans.

We refer to the variables that are varied dynamically throughout a scenario as short-term variables. One of these variables is vigilance, which is construct and which we take to be synonymous with attention, alertness, arousal, and emotional state. Vigilance will be modeled as beginning with a value that corresponds to an individual's motivation (long-term variable) when he goes on duty and will decay with time. In addition to decaying with time, an individual's vigilance can be discontinuously stepped to a higher value by an alerting response to a stimulus. The magnitude of an alertness step will be randomly drawn from an appropriate distribution. If the stimulus results in an orienting response, a maximal alertness step will be taken and the decay rate will be slowed by increasing the time constant.

Fatigue, as mentioned previously, is also a dynamic variable. We intend to model a fatigue index in terms of the concentration ratio of lactic acid to muscle glucose. This index will also account for the exchange rate of waste (excess) body heat with the enviornment and the effect of adrenaline. A pulmonary-cardio model of volume rate of oxygen, carbon dioxide, and heat transport will be described as a function of the fatigue index, physical condition, and acclimation. The model will be a lumped parameter set of coupled differential equations that relate the rate of work output (power expended) to the buildup of lactic acid (use of muscle glucose) and to the release of heat. Heat will be carried from the body by radiation, by convection/evaporation, and by respiration. The formal organization of the model will incorporate the physical parameters not as their "best known" physical chemistry values, but rather to give the best data fit to a military population.

The dynamic model of sensory adaptation will allow an exponential relaxation of detection threshold from the time at which the last intense source was sensed. A similar set of time constants will provide for recovery from dark adaptation levels to a brighter/more noisy environment to keep the sensory dynamic range within realistic limits.

Workload will be modeled as the degree of saturation of short-term memory capacity. Stimuli presented to an observer are serially placed into short-term memory in order of presentation. Stimuli can be of two types: those related and those unrelated to the scenario. Scenario related stimuli will be generated naturally by the model. Unrelated stimuli, "zilch" stimuli, will be generated as a Poisson process where the average presentation rate is user specified as a function of area on the ship.

All of the dynamic variables mentioned above will be used in decision making--that is not to say that an individual consciously accounts for these variables, but that they contribute to his subjective state. Knowledge will consciously enter into decisions. Knowledge will be the sum of initial knowledge, for which the modeled human will have perfect recall, and acquired knowledge about his personal experiences in the scenario and facts communicated to him. Recall of acquired knowledge will be probabilistically determined.

Other dynamic variables that will affect the subjective state are the individual's perceived threat to himself, his perceived threat to the system (or his purpose), and his perceived immediacy of the threat. These will all be evaluated as Bayesian evidence functions.

The basic human function model we envision is shown in Figure 1. It may be surprising that "detect," "search," "classify," "decide," etc., are not listed in Table 1 as human functions. They are missing because information gathering and recognitive tasks are considered to be potentially part of all the human functions of interest.

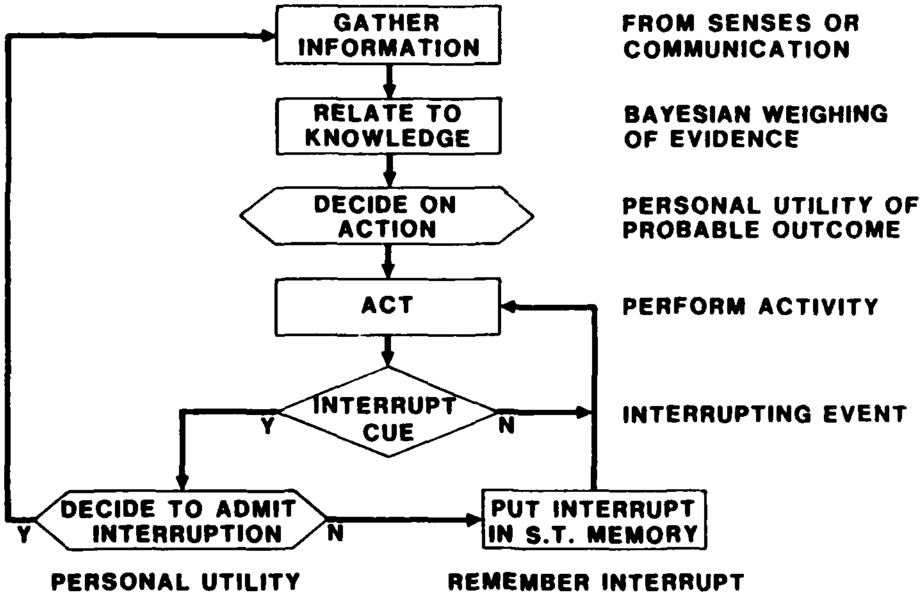

GATHER INFORMATION
FROM SENSES OR COMMUNICATION
RELATE TO KNOWLEDGE
BAYESIAN WEIGHING OF EVIDENCE
DECIDE ON ACTION
PERSONAL UTILITY OF PROBABLE OUTCOME
ACT
PERFORM ACTIVITY
INTERRUPT CUE
Y
N
INTERRUPTING EVENT
DECIDE TO ADMIT INTERRUPTION
Y
N
PUT INTERRUPT IN S.T. MEMORY
PERSONAL UTILITY
REMEMBER INTERRUPT

Figure 1. Basic human function model flow diagram.

The flow chart in Figure 1 appears to be an infinite loop; it should be viewed instead as an infinite spiral. The generalized model of human performance begins by adding new facts to the store of knowledge; recalling and correlating previously obtained knowledge with these new facts; deciding on a course of action, which could be to do nothing; and performing that action. That action will continue until it reaches its natural conclusion (which is not explicitly shown in Figure 1, but may be considered as a type of interrupt) or until an interrupting stimulus occurs. If an interrupt cue is present, the individual has to make a simple decision among three alternatives based on the type of cue and his activity. He may ignore the cue and continue his activity, remembering that the cue occurred. He may choose to delay responding to the cue for a short interval. He may respond immediately to the cue. If he decides to admit the interruption, he returns to a gather informaton stage with respect to the interruption. For certain types of interruptions he has no option; he must respond. For example, suppose that the telephone line is severed during a report given over the telephone or that the person receiving the report is interrupted. In either case, it is silly to continue reporting.

The human behavior/performance model will be implemented in a modular, event-sequenced, simulation code structure. MRC has successfully applied this simulation technique to problems as diverse as antiballistic missile defense, satellite communication, forest fire growth and suppression, and physical security of fixed nuclear weapon storage sites. Events that drive the simulation are held in time order on an event list. The simulation manager "pops" the next event from this list and, through a table lookup procedure, obtains the sequnce of modules to be executed to effect the occurrence of the event. The modules themselves are called into action by the simulation manager but do not communicate directly to each other. They can modify the data base and insert new events on the list. Maintaining this strict doctrine allows modules to be added easily or modified to provide alternate levels of detail. Each module has simple interface requirements and cannot interfere with other modules.

In summary, we would like to point out that on shipboard the sensing functions are mainly done by human patrols. Questions such as "What security benefits can be expected by adding sensor X to the system?" or "What is the relative advantage to security from installing system X rather than system Y?" will be addressed by a larger program at the Naval Surface Weapons Center, White Oak. This program includes the development of a computer simulation of the total security system, which will incorporate results of the model we develop.

This program also includes the construction of a physical simulation facility. Simulation predictions will be validated by experiments in the facility. Once validated, the computer model will be a tool for interpolation between the data points obtained from completed experiments and will also offer a means to economically explore system performance beyond completed experiments.

The obvious goal of a security system is to protect high value assets against a set of postulated threats. Threats vary considerably in magnitude, in objective, in determination, and in tactical approach.

Traditional security systems operate by reaction to an attack. The Navy Personnel Research and Development Center (NPRDC), which is in San Diego, will use the human behavior model in a stand alone mode in parametric studies of scenarios. NPRDC foresees using the model as the heart of an interactive security training simulator. In an interactive gaming mode, one (or more) of the simulated individuals would be replaced by a subject(s) at a terminal(s).

This paper has focused on the last task completed in Phase A of the contract. This task defines the design specification for the model software--the model's skeletal framework. In creating this framework, it is necessary to conceptually solve all of the problems that arise in the attempt to model human behavior. All humans in the scenario dramas share the following characteristics: They gather information from personal perception and by communication; they relate newly acquired data to what they can remember, accumulating evidence (in a Bayesian sense); they make decisions based on personal utility and perceived probability of an outcome (given a candidate response and their perception of the state of the wor,d); and based on these decisions they perform certain actions.

Some Human Factors Aspects of Military Entry Control Systems

by

Lt Jeffrey Woodard, Lt Joseph Nelson, and Dr. Bruno Beek
Rome Air Development Center
Griffiss AFB, NY 13441

and

Mr. Thomas Midura, HRA Associates, Inc., Burlington, MA

The Rome Air Development Center (RADC) is responsible for developing the technology to be used in future military entry control systems. This research and development is being done in support of the Tri-Service Physical Security Systems Directorate, PSSD (formerly BISS), and the Defense Nuclear Agency. Because use of guards and card/badge-type systems have been determined to be inadequate for identity verification for entry control, RADC has been charged with developing Personal Identification and Authentication (PIA) technology which relies on personal attributes, such as speech, fingerprint, handwriting, and others. The purpose of this paper is to focus on some behavioral science aspects of these PIA systems. Some of the human factors issues which are discussed have been addressed for several years in technology development programs. Other issues have not been investigated but may be vital in the development of secure entry control systems.

The relative success or failure of PIA systems is often dependent upon two human factors: (1) the acceptance of the system by the user population; and, (2) the testing procedures employed. These factors are examined for a number of laboratory and field tests. Related to testing, is the use of the familiar Type I (user rejection) and Type II (imposter acceptance) errors as criteria for PIA system performance. These errors are discussed and examined closely to show how dependent they are on testing procedures and the definition used for each respective error. The final topic discussed is one in which little is known, how to most effectively configure PIA systems and human guards together in operational entry control applications. A number of possible configurations are discussed and some results of interviews with military security guards will be presented.

SOME HUMAN FACTORS ASPECTS OF MILITARY ENTRY CONTROL SYSTEMS

Lt Jeffrey Woodard, Lt Joseph Nelson and Dr. Bruno Beek
Rome Air Development Center (RADC)
Griffiss AFB, NY

Mr. Thomas Midura
Harold Rosenbaum Associates, Inc.
Burlington, MA

ABSTRACT

For the past several years, RADC has been developing technology for use in future entry control systems. This research and development has been done in support of the Defense Nuclear Agency and the Physical Security System Directorate (formerly the BISS SPO). The main thrust of this R&D has been in the development of highly reliable, automated methods of personnel identity verification. The technology that has emerged has been based on personal attributes such as speech, fingerprint, and handwriting to form the basis for highly accurate Personnel Identification and Authorization (PIA) techniques. Laboratory and field tests performed by RADC and other Government and private organizations have clearly underscored the need for the application of behavioral science and human factors engineering in the design, development, and testing of entry control systems.

The purpose of this paper is to discuss some of the major human factors aspects associated with military entry control systems. This discussion will focus on the man-machine interaction between security guards, users, and imposters with entry control systems. It is these interactions which can strongly influence the overall security of an entry control system, the acceptability of the system to users, and the likelihood of penetration attempts.

INTRODUCTION

In early 1972, the Air Force was assigned the role of executive agent for all Research, Development, Test and Evaluation of external physical security equipment for DoD. This initiated the formulation of the Base and Installation Security System (BISS) program. The task of developing the next generation PIA technology was undertaken by BISS; at that time it was felt that a fully automated system for moderate to high security would only be practical if based on the utilization of ineradicable personal characteristics. Coded ID systems (i.e. coded cards, memory) while thought to provide significantly low error rates and considerable resistance to code breaking, were relegated to low security applications, because of their susceptibility to duress situations. Mitre was subsequently tasked to survey potential PIA techniques for BISS applications which could be placed into prototype development. Speech, handwriting, and fingerprint verification systems were selected as having the greatest potential and advanced development was initiated.

Since the initial selection of the three prototype techniques, the expanding commercial market for security equipment for intruder detection, computer security, illegal alien control, electronic funds transfer, and forensic applications have attracted additional investigations into the field of entry control technology. Many new techniques and significant improvements in known techniques in PIA have been developed resulting in a broader technology base to support the DoD BISS entry control requirements and also a substantial body of literature in the field. Probably the technique which has received the most attention has been in the area of speaker verification. The speaker verification system performed the best of the three systems tested by Mitre, and is currently undergoing engineering development by the Air Force Electronic Systems Division (1). This speech verification system was initially developed by RADC as an extension of its speech recognition work. Because of the substantial body of work in the areas of speech and speaker recognition for military and commericial applications, speaker verification has been a rational selection for PIA use. Also, because of the long history of forensic technology investigations, handwriting and fingerprint verification techniques have received a great deal of attention. Thus, these three techniques have dominated the military and open literature, and have been the subject of ambitious R&D. The use of "voiceprint" and "signature" verification by subjective visual comparisons have pretty much been discarded in favor of real-time signal processing of speech and handwriting dynamics. With the emergence of high speed optical scanners and substantial reduction in computation costs, static attribute systems such as fingerprint and hand geometry have also discarded direct cross-correlation techniques for digital signal processing and holographic techniques. Newer techniques such as EKG, body vibration, and retinal patterns are still in early stages of development but offer considerable promise for the future.

This paper presents an analysis of some human factors of military entry control systems. It should be emphasized that the requirements of military entry control systems are diverse. There are major inter and intra-service differences. The size, location, function, and environment of each military installation is unique. Other variables, such as types of resources protected, number of secure areas, population size, throughput requirements, and others may also be different for each individual installation. Thus, any analysis of the human factors involved is complicated by the wide variation of requirements and characteristics of DoD bases and installations.

The paper is organized into three sections. The first describes how PIA devices and techniques are used in entry control systems. The second discusses the importance of user acceptance in the operation of entry control systems. The third section presents a theoretical analysis of problems encountered in the use of accuracy measures of PIA techniques. Some of these human factors issues are fairly well known; others are not and should be subjects for future research efforts.

THE USE OF PIA TECHNIQUES FOR ENTRY CONTROL

THE ENTRY CONTROL SCENARIO

The objective of any entry control system is basically simple - allow authorized personnel access into a protected or secure area with a minimum amount of inconvenience and prevent unauthorized personnel from gaining access. In practice, the objectives may be more complicated. For example, in some instances it may be desired to entrap or detain unauthorized individuals in a detainment booth, area, or module, if they are detected attempting to gain access. Many current military entry control systems require verification of identity on egress as well as ingress. At some installations, it is necessary to check individuals attempting access for contraband on egress, ingress, or both. Some facilities have a fairly steady flow of pedestrian traffic during a working day, while others have peak periods where throughput requirements become very high. But regardless of the specific procedures and characteristics of the system, the key to any entry control system is the use of an accurate method of identity verification.

WHY PERSONAL ATTRIBUTES?

Verification decisions are made on an entry control system by an analysis of an attribute possessed by the entrant candidate, and by a comparison of the attribute with previously stored information. Attributes can be classified as being one of three types: personal, which are ineradicable characteristics; artifacts, which are objects that can be carried by an individual such as a badge; knowledge-based, which are codes, symbols or combinations which can be recognized or memorized. The vulnerability of identity verification based on artifacts or knowledge - based attributes is well established. These attributes are subject to theft, forgery, duplication, alteration, destruction, etc. Perhaps more importantly, individuals who use them are susceptible to various types of duress-extortion and blackmail or collusion. In general, these attibutes are not unique and may be easily transferred from one person to another.

Guards have traditionally been and will continue to play an integral role in entry control. However, when guards are given sole responsibility for identity verification decisions, they are also vulnerable to duress and collusion. In addition, the accuracy of humans performing visual comparisons for identity verification is unknown, but there is evidence to suggest that their ability to recognize people is limited (2). This inherent limitation can be amplified by boredom, stress, fatigue, and other physical or emotional problems. Generally, guards perform verification by comparing entrant candidate facial features with a picture badge, stored video image, or color photograph. The comparison can be done live or over a television monitor. Basically, the problem with guards performing identity verification is the same problem shared by visual "voiceprint" analysis - it is subjective.

Personal attributes can offer the greatest potential in accurate identity verification. Personal attributes are, in general, unique to an individual and are very difficult to duplicate, alter, destroy, steal, or transfer from one individual to another. Basically, PIA techniques which rely on personal attributes obtain a set of measurements from an individual at the time he attempts to gain access, and compares that set of measurements with a set of measurements that were obtained from the same individual at an earlier enrollment or "learning" session. Let this set of measurements be denoted by the vector $\underline{x}$. Thus $\underline{x}$ might be, for example, the relative amplitude spectrum obtained by a speech verification system or the signature dynamic data obtained by a handwriting verification system. Whatever the characteristics, $\underline{x}$ is subject to intrinsic variations for any given individual. In addition, there are some variations produced by the PIA system itself (e.g., orientation in fingerprint systems). During the "learning" phase, a number of measurements, $\underline{x}_1$, have been accumulated on the individual, I_1, and at least in principle, a density function, f(x), has been obtained which indicates the relative frequency of the measurements. Suppose now that $\underline{x}_2$ is obtained from another individual, I_2, who attempts to enter as I_1, and is processed through the system. The objective of the entry control system is that the individual I_2 should be rejected. If $\underline{x}$ were unique for each individual, then no problems would arise in the verification process.

For purposes of exposition, assume that the population consists of two individuals. Further, let the density of $\underline{x}_2$ for the second individual, I_2, be g(x). The problem for the entry control system is to verify that the first individual, I_1, is the authorized entrant when, indeed $\underline{x}$ was obtained from him and to reject the second individual on the basis of $\underline{x}$ obtained from him. What is sought is a decision function d(x) which decides to admit the entrant whenever $\underline{x}$ falls in a region R_1, and to reject the entrant whenever $\underline{x}$ falls in R_2, i.e.,

$$d(x) \quad \begin{array}{l} \text{Admit if } \underline{x} \in R_1 \\ \text{Reject if } \underline{x} \in R_2 \end{array} \qquad \text{(eq 1)}$$

A decision to verify the second individual when in fact he should have been rejected is termed a Type II error. A decision to incorrectly reject the first individual is called a Type I error. These two errors will be discussed in further detail in a later section.

CLASSIFICATION OF PERSONAL ATTRIBUTES

In a previous report, personal attributes have been somewhat arbitrarily classified as either static or dynamic (3). Dynamic attributes can further be classified as learned or physiological. Static attributes can be thought of as external to a human, such as fingerprints, palmprints, and retinal patterns. Static attributes appear to be very stable over long periods of time, but can display considerable short-term variability (such as a cut or nick on a fingerprint). Dynamic attributes are time-varying analog signals which can be transduced electrically or mechanically. In general, dynamic attributes can exhibit significant long-term variability. Long-term variability in many cases can be accommodated by adaptive updates of user reference data, such as is currently done on the speaker verification system (4). Physiological dynamic attributes are external or internal physical processes which generate signals without conscious effort by an individual. Examples of this attribute are electrocardiograph (EKG) signals, electroencephalography (EEG), and ballistocardiographs. Learned dynamic attributes are also based on internal or external processes but which require a conscious activity or effort by the individual. Examples of such attributes are speech and handwriting.

Two other classification criteria are useful in discussing personal attributes. One is the intrusiveness of the attribute. Intrusive attributes are those that reveal or expose some normally sensitive or private bodily process or anatomical part; unintrusive attributes do not expose sensitive bodily areas. A second useful classification criteria is the passiveness of the attribute. Passive attributes do not require any conscious action on the part of the individual, while active attributes do require some conscious activity. Note that in general static attributes tend to be passive and unintrusive, while dynamic attributes tend to be active and intrusive. Table 1 below is a chart which classifies some personal attributes according to the scheme previously discussed. Again the classification scheme is somewhat arbitrary, and the table does not include all possible personal attributes.

	STATIC		DYNAMIC			
	PHYSIOLOGICAL		LEARNED		PHYSIOLOGICAL	
	INTRUSIVE	NOT INTRUSIVE	INTRUSIVE	NOT INTRUSIVE	INTRUSIVE	NOT INTRUSIVE
ACTIVE	SALIVA, BLOOD AND URINE ANALYSIS		QUESTION AND ANSWER	SPEECH HANDWRITING TYPING STYLE	LIE DETECTOR BITE PATTERN	
PASSIVE	RETINAL PATTERNS ULTRASONIC	FINGERPRINT HANDPRINT PALMPRINT HEIGHT/ WEIGHT FACIAL FEATURES VEIN PATTERNS			EKG EEG PPG BALLISTOCARDIOGRAPH BLOOD PRESSURE	BODY VIBRATION BODY RESISTANCE BODY TRANSFER FUNCTION

TABLE 1 CLASSIFICATION OF PERSONAL ATTRIBUTES

USER ACCEPTANCE

The use of automated PIA systems in the future and their satisfactory performance will depend heavily upon the motivation of those required to use it on a daily basis. For maximum effectiveness, PIA systems should be acceptable to those people. Certain attributes such as signature, fingerprint and even voice have been considered acceptable means of personal verification for some time. However, the use of many of the newer attributes, especially those that may involve invasive transduction techniques may well meet with great reluctance by future users who consider any form of entry control (and personal ID) an invasion of their privacy. Although military user populations may have less choice than civilians regarding their desire to use PIA systems, their cooperation is nevertheless crucial in determining the effectiveness of the system. In general, there is a tradeoff between user acceptance and security; thus, whatever PIA systems are used will cause some user dissatisfaction.

PREVIOUS STUDIES

User acceptance can be thought of as the amount of pain, embarrassment, anxiety, discomfort, or inconvenience perceived by individuals as being caused by a PIA system. From previous PIA field tests and user surveys, several recommendations have been made concerning user acceptability. One recommendation is that the PIA device must be timely, not only to reduce user impatience but also to meet operational throughput requirements. Substantial user frustration can occur if long queueing lines are formed, either because of long verification times or by repeated Type I errors. A related problem is the question of what procedures to take with users who are incorrectly rejected access, i.e., Type I errors. This will be addressed below under the section on hybrid systems. Another recommendation concerns enrollment or learning sessions used to generate and file users' attributes reference data. Enrollment sessions can be a source of user dissatisfaction if they are long and tedious. The enrollment sessions should also be used to gain user cooperation, reduce apprehension, and increase motivation about using the system.

In a study of potential PIA techniques, twenty-one people were asked to rate a number of different attributes for acceptability. The result of this study indicated most subjects preferred attributes which were inherently passive, unintrusive, fast, did not involve the use of electrodes (as in EKG), and did not involve the use of the face, ear, or head. (5) In another effort, a field test was conducted to determine the effectiveness of three PIA systems using voice, fingerprint, and handwriting, respectively. A survey was performed at the conclusion of the field test to investigate user attitudes towards the three sysѡems. The results of the sixty-four subject survey were that fingerprint was preferred most, handwriting next, and speech the least (6). This result m'ght be expected considering fingerprint is passive while speech and handwritıng are active attributes. There were several other interesting observations that were determined from the survey. One was that despite the fact that it was the least preferred, the speech verification system performed the best. Another observation was that many of the negative feelings for voice stemmed from the fact that most people were inexperienced and slightly uncomfortable in interacting with a computer. In this case, people had to both listen to computer generated prompting phrases and then repeat those phrases back to the computer. A number of comments made by users pointed out the difficulty of understanding some prompting phrases, about feeling uncomfortable speaking into a microphone, and about the impersonal and "cold" manner of the prompting voice. A final observation that was made concerned the importance of the booth or module used to house the speaker verification system. A number of negative comments were made by users about the booth; the fingerprint and handwriting systems were not similarly housed in booths and this may account for some of the negative feelings about the voice system. Thirty-four percent of the subjects of the field test said that they did not feel comfortable in the detention booth. Some people felt the booth was too small, in fact, one subject refused to enter the detention booth at all because he felt it was claustrophobic. The fact that the doors locked behind a user when he entered the booth was intimidating to some subjects.

BOOTH DESIGN

Human factors considerations are important in the design of entry control booths and modules, as evidenced in the discussion above. Entry control booths of the future may have to incorporate a large variety of electronic, optical, and other equipment. This equipment will be used to perform such functions as: PIA for identity verification, floor scales for personnel weight measurement, closed circuit television and two-way audio channels, metal detectors, explosive detectors, and nuclear material detectors. The entry control booths must be engineered so that the equipment can function as a unit in an effective manner without causing undue apprehension or inconvenience to the people who must use them. The booth may also serve as an aid in detecting potential intruders using physiological measures or in detecting persons who may be under stress.

CONCLUSIONS ON USER ACCEPTANCE

The attitudes of users will play as important role in the wider acceptance of PIA devices. Regardless of what attribute is used, it is likely that some individuals simply cannot or will not use it. Some individuals do not care to use fingerprint PIA devices because it has criminal (FBI, etc) connotations for them. Others will not want to use an EKG device because of a fear that medical ailments may be diagnosed or revealed, or from fear of electric shock. Other individuals will not be able to use handwriting devices because they are unable to sign their name consistently, either because of nervous disorders or large variability in writing styles. The ideal personal attribute of the future will be one which is essentially transparent to the user, that is, the user will simply walk in a booth or area, and out again without performing any actions or without being aware of any measurements being taken. But for the present, studies are needed to collect ergonometric and behavioral data which can aid in determining what people are physically or psychologially unable or unwilling to use.

TYPE I AND TYPE II ERRORS

In considering the accuracy of PIA devices or systems, the familiar terms "Type I" and "Type II" errors are often used. Type I error is used to describe the PIA decision where an authorized user has been incorrectly rejected. Type II error is used to describe the PIA decision where an unauthorized person, or imposter, is incorrectly verified as an authorized user. In practice, these error rates are used as measures to evaluate the accuracy of various PIA systems in laboratory and field tests, for comparative evaluation of two or more PIA systems, and for a measure of entry control system security. Unfortunately, the interpretation of Type I and Type II errors is dependent on assumptions made, the testing conditions, the population used during the test, and other variables. Hopefully the following discussion will attempt to define more precisely Type I and Type II errors and point out some of the problems in interpreting published test results. A section on hybrid systems is presented which shows how both types of errors may be reduced by combining two or more PIA systems together.

THEORETICAL DISCUSSION

Referring again to the discussion preceding equation 1, implicit in the decision is the existence of penalties or losses for making the wrong decision. That is, there is a cost, C_1, associated with deciding not to admit, when the entrant is the authorized first individual, and a cost, C_2 associated with failing to reject the second individual. The risk associated with the first decision is the expected value of the loss, given the entrant is the first individual:

$$\text{Risk}_1 = E(C_1) = C_1 \int_{R_2} f(x)\,dx \qquad \text{(eq 2)}$$

The corresponding risk for the second decision is:

$$\text{Risk}_2 = E(C_2) = C_2 \int_{R_1} g(x)\,dx \qquad \text{(eq 3)}$$

In general, one desires to minimize the total risk; however, this is in general not possible. For example, if prior probabilities that the entrant is individual 1 or individual 2 were known then the total risk could be written.

$$R_t = \pi C_1 \int_{R_2} f(x)dx + (1-\pi) C_2 \int_{R_1} g(x)\,dx \qquad \text{(eq 4)}$$

where π is the prior probability that the entrant is individual 1.

The objective is to choose the regions R_1 and R_2 so that R_t is minimized. This is the Bayesian approach to the problem and it is accessible when prior probabilities are known. In the absence of such knowledge, alternative criteria are the minimax (choose R_1 so that the *maximum risk is minimized*) and the maximum likelihood (decide to admit whenever $f(x)/g(x)$ C_2/C_1) approaches, among others.

The method of hypothesis testing, as applied to the present example, is to fix the probability of incorrectly rejecting entrant 1 (Type 1 error) while minimizing the probability of admitting entrant 2 (Type II error). This method is only appropriate when prior probabilities are lacking. If such probabilities are available, then the risk or expected cost can be significantly reduced.

To return to considerations that apply to real world PIA, there are several ramifications to the above analysis. First, the population of alternatives is not restricted to one individual. It is, for all practical purposes, infinite. Thus, each impostor has an associated g(x) which is not necessarily known. In this respect the testing more closely resembles the classical statistical problem of determining whether the set of measurements comes from a given, known distribution. Second, the costs or penalties of a given decision procedure are functions of the total system in which the PIA is imbedded. For example, the throughput is an important parameter that interacts with the Type I and Type II errors on a global scale. Third, the analysis above applies to the "casual" impostor who does not possess technical knowledge of the system or special resources that would assist him in spoofing the PIA. Such considerations as the last are device specific and cannot be resolved analytically.

First, let it be said that there are three contexts that warrant different evaluations of the Type II error. There is the "casual" Type II error which results from inadvertent actions on the part of the users. This can occur, for example, when an entrant mistakenly and unintentionally uses the identification number of another valid user. Second, there is the deliberate attempt to enter under an assumed identity but without the use of technical "spoofing" aids. This can occur when a valid entrant at a particular security level attempts to "ape" (such as a voice mimic or signature forger) another entrant with a higher level. Other situations include the cases where users are in a jocular mood, for one reason or another, and attempt to foil the system. The third context involves the use of technical aids and probably requires a high level of sophistication on the part of the impostor. This partition of the possible contexts wherein false acceptances can occur is somewhat arbitrary since the actual case is a continuum of possibilities. Such a subdivision is useful, however, if to establish guidelines in the detailed study of the problem.

For any analysis of the performance of a single PIA system or hybrid system it is essential that reliable Type I and Type II errors be obtained from the empirical data acquired during the "learning" phase of the program. The form that these reduced data take must correspond to the function that the decision making system will perform when in operating condition. It was pointed out previously that the filter associated with a particular user is used on measurements obtained on <u>one</u> impostor in a given operational situation. That is, the test is not performed on an <u>average</u> impostor but on a specific individual. For a particular threshold (determined, say, by fixing the Type I error) each impostor and the measurements associated with him will have a unique Type II error. The method of calculating the Type II error by the formula:

$$\text{Type II error} = \frac{\text{Number of False Acceptances}}{R}$$

where R is the number of verification attempts over the whole population, therefore assumes that the impostor distributions are identical, or at least similar enough to permit the use of the formula. The same is true when the Type II error is computed by the formula:

$$\text{Type II error} = \frac{\text{Number of False Acceptances:}}{bM\ (M-1)} \qquad \text{(eq 5)}$$

where b is the average number of test files generated per user and M is the number of users. This may be seen by observing that

$$b = \frac{1}{M} \sum M_i \qquad \text{(eq 6)}$$

where M_i is the number of files generated by the ith user. Then the total number of trials is given by

$$M_t = \sum_{j=1}^{M} \sum_{i \neq j} M_i = \sum_{j=1}^{M} [\sum M_i - M_j] = bM(M-1) \quad \text{(eq 7)}$$

The difference between the two methods of obtaining the Type II error is that, in the first case the computation is based on a population consisting of both users enrolled in the system and non-users not enrolled. In the second case the population consists of users only. In either case the Type II error is calculated for the average impostor. The extent to which either calculation is appropriate is a matter for statistical examination and cannot be answered without recourse to the data from the particular PIA involved. It may be noted, however, that in the second case, use of reference files may have serious drawbacks with certain PIA techniques. For example, Type II error rates for the AHV system were previously computed by comparing samples of enrolled users' handwriting dynamics while signing their own names to each others' reference files. While this may provide a reasonable estimate of Type II errors resulting from inadvertent entry errors (or frivolous impostors), these rates are hardly representative of those associated with a concious intruder of even the "casual" type with knowledge of just a valid user name. Most PIA techniques, however, do not exhibit this peculiarity, and the problem reduces to the degree the imposter population is represented by the reference file population.

A similar problem exists with respect to using comparison of reference files to generate Type II estimates for voice verification system such as the adaptive system developed by RADC. Because the system is adaptive, the reference data of users is updated with each successful verification and as a result represents an average utterance, not any single utterance. Because it is an average, it is not clear what significance can be given to matching data in this form for two users. Also, the time- registration of reference data would be insignificant because exactly the same number of matrices are stored for all user reference files. Since the parameters of actual speech utterances vary, achieving or not achieving matches between reference files has no meaning (7).

It should be clear from the above that in general, the average error computed above does not correspond to the actual Type II error probability of any particular decision process. It is an estimable parameter; but, it does not relate directly to the probability that an impostor can breach the system.In particular, when the meaning of the Type II error is scrupulously examined it is seen that, for many situations, a Type II error is costly, then the estimation of its probability cannot be made on an average basis. The same may be said for the Type I error probability. For example, let the number of users or valid entrants for a given installation be denoted by M. At least twice each day the same M user's will be candidates for ingress or egress. An average (Type I error probability) cannot be used to assess throughput and other system implications since the range of Type I errors associated with individual entrants may be large.

Particular attention to the use to which the estimates will be put is necessary. A determined impostor, with or without sophisticated technical aids, poses the main threat to such a system. To be able to make meaningful statements about the probability that such an impostor can deceive the system requires a rigorous estimation procedure.

The minimum requirement for a system analysis is the set of operating characteristic curves for each entrant. These curves give the Type II error probability versus the Type I error probability. This is especially necssary to implement the combinational logics for hybrid systems. If the results of the analysis are to be meaningful, the confidence which can be placed in the statistics must be ascertained. It is, of course, possible to assume distributions for the pertinent quantities and to perform parametric studies. Such an approach, however, can lead to useful results only if a datum or reference case of practical interest serves as a point of departure.

For the purpose of establishing a reference case, an in-depth analysis of the data acquired on a limited number of entrants can be used. A useful procedure would be to determine fits of these data to some parametric class of distributions (Pearson, Gram-Charlier, etc.). Having established the class of distributions, parametric studies can then proceed.

It is doubtful that sufficient data exists to perform the analysis indicated in the above. This is a consequence of the current methods of estimating Type II errors. The estimation properly proceeds by determining the distribution of the decision variate for a given impostor.

Moreover, the decision logics employed in many contexts involved adjusting thresholds on successive attempts (sequential decision strategies) thus, further complicating the situation. In any case, before attacking the general systems analysis problem, it would appear that a detailed analysis of a limited population is warranted. Such an analysis can lead to a more rational assessment of the Type II error vulnerability of the verification system.

HYBRID SYSTEMS

As was seen in the previous section, even when the measurements from a given PIA are optimally processed, a decrease in a (Type I error) generally entails an increase in B (Type II error) and vice versa. Improvements in a or B that are confined to a single PIA will impact the throughput of the global system. This fact suggests the use of a combination of two or more PIA techniques in OR-logic or AND-logic modes (8). Generally, use of OR-logic will reduce the Type I error again, increasing the Type II error. Similarly, AND-logic will reduce the Type II error while increasing the Type I error. The problem is to assess by how much such modifications affect these errors; and, more importantly, the total system effect of the hybrid processes. In addition to the logical combination of PIA techniques possible, one can alter the physical location of each of the PIA techniques comprising the hybrid system to achieve different desired impacts on system throughput. Typically, combinations of identifier elements have been thought of being housed in the same control element (enclosure/detainment device). An attractive alternative (from the perspective of system throughput) would be to house each identifier in its own control element. In the sequential identification process, branching would occur on the basis of the results of the first identifier, either immediate entry, or proceed to the second identifier, thus freeing the first identifier for further processing of the entrance queue. For example, minor degradation of the Type I error may be acceptable if the throughput is sufficiently increased. The throughput in this case can be improved if use of AND-logic reduces the type II error. Moreover, by modifying the decision logic in the first system the second system may function as a filter, out of the main flow of traffic. Thus, the first system decision structure could be modified to produce the following output:

$$f(x)= \begin{array}{ll} \text{Admit:} & X \in R_1 \\ \text{Reject/detain:} & X \in R_2 \\ \text{Further inquiry:} & X \in R_3 \end{array} \qquad \text{(eq 8)}$$

The region R_3 is is a penumberal zone where a clear-cut decision is not possible. When the data fall in this region, the entrant is moved to another queue and the second PIA which measures a generally different human characteristic. In this way throughput may be increased and both the Type I and Type II errors decreased. This procedure is commonly used in statistical analysis where it has proven useful. In effect, it is a form of randomization of the decision process.

Some idea of the systems implications of using two PIA in an OR-logic mode can be gained by the following exercise. Let a_1 and B_1 be the Type I and Type II errors resulting from PIA I, and a_2 and B_2 be the corresponding errors for PIA II. Then the combined system errors are:

$$a \simeq a_1 \ a_2 \qquad \text{(eq 9)}$$

and

$$B = 1 - (1-B_1)\ (1-B_2) \qquad \text{(eq 10)}$$

Similarly for the AND-logic combined system errors are

$$\begin{array}{l} a \simeq 1 - (1-a_1)\ (1- a_2) \\ B = B_1\ B_2 \end{array} \qquad \text{(eq 11)}$$

If the operating characteristic curves for each system were known, and the thresholds accessible, the combined system can be optimized for a particular application. Choosing a system a or B, the other parameters can be minimized through selection of the appropriate operating threshold for each individual system. However, the physical configuration of the combined systems optimized in this fashion, will have a substantial impact on overall performance at the installation. The AND-logic system processes all entrants in system 1, detaining those who fail, and processes those who pass in system 2. The OR-logic system allows ingress (or egress) to those who pass in system 1 and tests only the rejects in system 2.

The question now arises: Which of the two systems should be used first in the testing sequence? In general this question does not have any easy answer since it is a function of: arrival rate of impostors, arrival rate of valid entrant, servicing time (verification) for each subsystem, cost (tangible and intangible) of delaying a valid entrant, etc.

Also, the question of imposter processing must be considered. What action is taken upon a rejection and what is its impact on other users? To examine these questions, a hybrid system simulation is being constructed which will enable the performance of various hybrid configurations to be evaluated for different traffic densities, error rates, and combination logics. This simulation will consider single and multiple queues, parallel portals, co-located or spatially separated PIA systems, detainment constraints, traffic flow protocols, and multiple logic configurations. A description of the simulation and some examples of different hybrid configurations are shown in the appendix.

CONCLUSION

Current work in behavioral science aspects of physical security systems deals with the characteristics of either the security force or the perceived adversary. We now have one more element to contend with, namely, the operational personnel of the base or facility for which the security system is designed to protect. We must better understand the role which non-security personnel play within the overall operation of the system. Clearly the use of automated PIA systems in the future and their satisfactory performance will depend heavily upon the motivation of those enrolled and required to use it on a daily basis. User acceptance of the PIA attributes selected is certainly an important factor. Another element for consideration in PIA attribute selection is the ease of training in the proper use of the system and the motivation for continued proper use on a long-term basis. Certainly there will be more latitude in selection of appropriate techniques where the security level is of paramount concern, such as the protection of nuclear assets. In other applications, however, it has been found that systems which add any delay to current entry procedures face many obstacles in their adoption. Surveys of possible areas of application of automated systems in the future have shown that personal recognition by a guard plays a dominant role, even in those areas where single badge systems are implemented. In some cases personal recognition must be relied upon to maintain an acceptable throughput rate during high traffic periods. In addition, certain high level personnel (VIPs) simply will not tolerate any additional delays, simply for the purpose of identity verification.

Another concern is the longterm performance of automated systems using the PIA attributes mentioned previously. A further observation is made on the use of an "average" Type I error rate as a performance measure. This metric will certainly provide useful information on relative performance of different PIA systems since it is based on a common data base of population signatures. However, when assessing the attractiveness of various attributes/PIA techniques, it is desirable to know sensitivity to long and short-term variability.

Longterm variability in most cases can be handled by adaptive updates of the system. The necessity to do this, however, can only be determined from an examination of the population data. This data base however, simply does not now exist.

Consideration for the establishment of a physical security ergonomic data base should include the need for PIA attribute characteristic data. This data should include statistics on longterm and short-term variability, diversity of the signatures across the user population, that is, separability, and any degree of correlation which may exist between attributes that may impact error rate performance. Since, in considering the use of hybrid systems it is desirable to obtain individual operating characteristic data, it is evident that sample size considerations may severely limit the number of attributes that could be contained within such a data base.

There has been considerable research in analyzing potential adversaries to security systems. Most of these studies have focused on the analysis of the threat to US nuclear programs. These studies have included a categorization of potential adversaries into classes such as terrorist, criminal, psychopath, intelligence agents, etc., a characterization of each class based on demographic data such as sex, race, age, and others, and an estimation of likely strategy and tactics, goals and objectives, willingness to take risks, and motivational factors. Although these studies may be applicable to US nuclear programs, it is likely that they are not appropriate for characterizing potential advesaries to other military high-security installations. The goals and objectives of adversaries to communications sites or computer facilities may be entirely different from those to nuclear weapons storage areas. New studies are needed to attempt to understand better the nature of the threat to these non-nuclear high-security assets.

APPENDIX

An entry control system (ECS) consists of entry points or portals used upon entrance and/or exit from an installation. Associated with each portal are one or more Identity Verification (IV) devices (e.g. voiceprint) which may be common to other portals. Figures 1a, 1b, and 1c depict entry control systems of 3 and 4 portals with and without common IV devices ("A", "B", and "C"). These devices may be used in different "OR" logic or "AND" logic combinations and may be housed within either a common enclosure or a number of separate enclosures. In the latter case, there may be queues of variable or limited length between the detection modules.

The purpose of this simulation is the estimation of the performance measures of throughput, waiting times, queue length, and device utilization. The difficulty of the simulation is great variety of possible configurations for an ECS. It therefore, will be useful to breakdown an ECS into more basic component parts or subsystems.

The basic subsystem for the simulation is what will be called a single "portal system". A "portal system" will be defined as the entrants and all the processes the entrants may be subjected to upon entering a single portal. For example, under the assumption that the "BRANCH" in Figure 1a is unbiased, the system depicted there contains three identical portal systems. Similarly, if we assume in system 1b (Figure 1b) that queues 1 and 3 are identical and the "BRANCH" unbiased, the portal systems of portals 1 and 3 are equivalent. System 1c consists of four very dissimilar portal systems (henceforth denoted by PS). A typical PS can be broken down as follows:

a. An arrival process in the form of some probability distribution (formula, graph or raw data)

b. An initial queue

c. A point of entry (portal)

d. One or more "IV units". It is necessary to restrict the term "IV unit" to an identification device which requires:

1. An approach process (eg. walking to, logging on).

2. Usage (eg. phrase repetitions, internal processing).

3. A decision which dictates the next destination of the user.

4. A departure process.

It should be noted that by the above criteria, a device which utilizes the statistics of more than one attribute, but only requires a single approach and departure is still considered as a single "IV unit" (denoted by IVU).

e. Restricted enclosures or booths. These detention modules typically contain an IVU that is not required. Occupancy is generally restricted to one person at a time for verified traffic which may also involve an escort situation. For unverified traffic, occupancy could be possible.

f. Intermediate queues connecting enclosures. These queues may be of limited length, involve different disciplines and priority structures.

g. Some form of detention whereby users rejected by an IVU may be held pending further investigation.

h. Intermediate portals.

i. A destination.

I. PORTAL SYSTEMS

A. Simple Models

A.1 One IVU (single direction): arrivals queue, enter E when unoccupied, use A, proceed to T upon acceptance, users exit or are detained. (Figure A.1.1)

A.2 One enclosure (a system without verification generally used upon departure). (Figure A.2)

A.2.1 Single service: arrivals queue, enter E when unoccupied, proceed to T (limited to single departures).

A.2.2 Bulk service

A.2.2.1 Arrivals queue, upon availability of E all members of queue proceed through E to T.

A.2.2.2 Same as above except only m users ($m \leq 2$) can proceed through at any one time.

B. "OR" Logic Models

B.1 Sequence Determined

B.1.1 Single enclosure (coincidental). (Figure B.1.1)

B.1.1.1 Arrivals queue, enter E when unoccupied, use A, proceed directly to T upon acceptance or to B upon rejection. Users accepted at B proceed to T, rejected users exit or are retained.

B.1.2 Double enclosure (sequential)

B.1.2.1 Arrivals queue, enter E1 when unoccupied, use A, upon acceptance proceed to T. Rejects advance to Q1, enter E2 when unoccupied, use B (binary), etc. (Figure B.1.2.1)

B.1.2.1a Q2 limited.

B.1.2.1b Q2 limited to m (m $\leq$ 1, typically 1).

B.1.2.1b1 Q2 limited by not allowing departures from Q1 until length Q2 m (E1 would be available for reverse traffic).

B.1.2.1b2 Q2 limited by not allowing departures from E1 until length Q2 m.

B.1.2.5 Same as B.1.2.1 without Q2. Breakdown is:

B.1.2.5a Departure from E1 only when E2 is unoccupied.

B.1.2.5b Departure from Q1 only when E1 through E2 is unoccupied.

B.2 Sequence Undetermined

B.2.1 Single initial queue: arrivals queue (Q1), enter the first available (unoccupied) enclosure, use the IVU, proceed to T upon acceptance. Rejects advance from A to Q2B or from B to Q2A and await to use next IVU. Successes to T, failures exit. A number of systems are possible depending upon the priority of Q2B and Q2A relative to Q1. (Figure B.2.1)

B.2.1a Q2B and Q2A have priority over Q1.

B.2.1b Q1 has priority over Q2B and Q2A.

B.2.2 Two initial queues. Similar to B.2.1. Not significantly different from B.2.1 unless the arrival population is divided into two groups which are required to use either IVU A or B first. (Figure B.2.2)

C. "AND" Logic Models

C.1 Single Enclosures (coincidental)

C.1.1 Arrivals queue, enter E when unoccupied, and must use A and B successfully to gain entry (T), otherwise are detained or exit. (Figure C.1.1)

C.2 Double Enclosures (sequential)

C.2.1 Arrivals queue and must use A and B successfully to gain entry. E1 and E2 are limited to one person at a time, and there is an intermediate queue, W2 (Figure C.2.1). The possible models follow the breakdown of B.1.2.1 concerning Q2, i.e.:

C.2.1a Unlimited length of Q2

C.2.1b1 Limited by departure from Q1

C.2.1b2 Limited by departure from E1

C.2.5 Same as C.2.1 with no intermediate queue.

SYMBOL TABLE

Q = QUEUE

□ = RESTRICTED ENCLOSURE

○ = IDENTITY VERIFICATION UNIT (I.V.U.)

→ = TRAFFIC FLOWS

⬡ T = DESTINATION OR TERMINUS

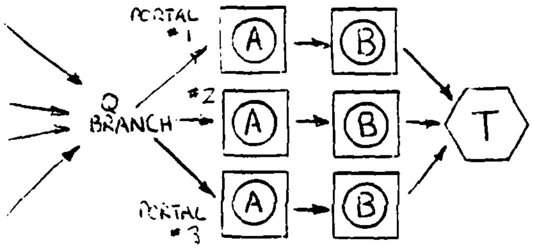


FIG. 1 A. "AND" LOGIC

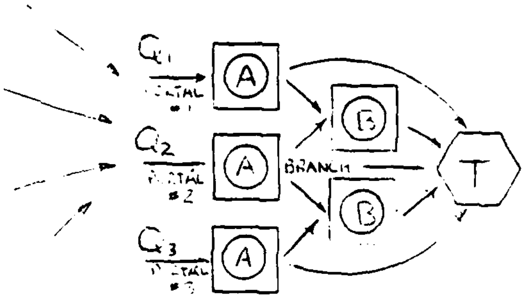


FIG. 1 B "OR" LOGIC

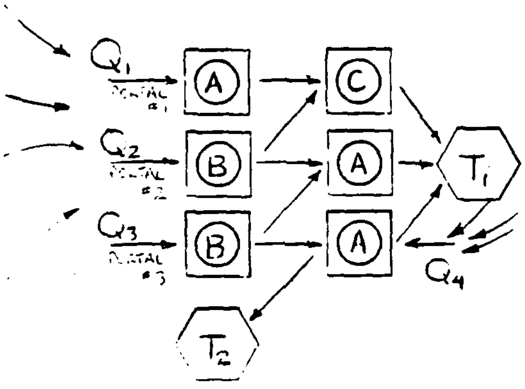


FIG. 1 C

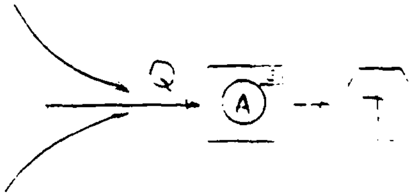


FIG A.1.1

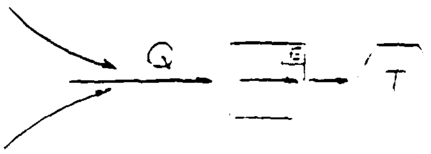


FIG A 2

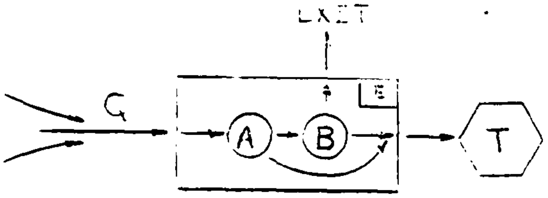


FIG B.1 1

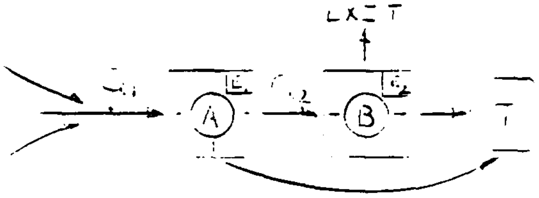


FIG B 1 2

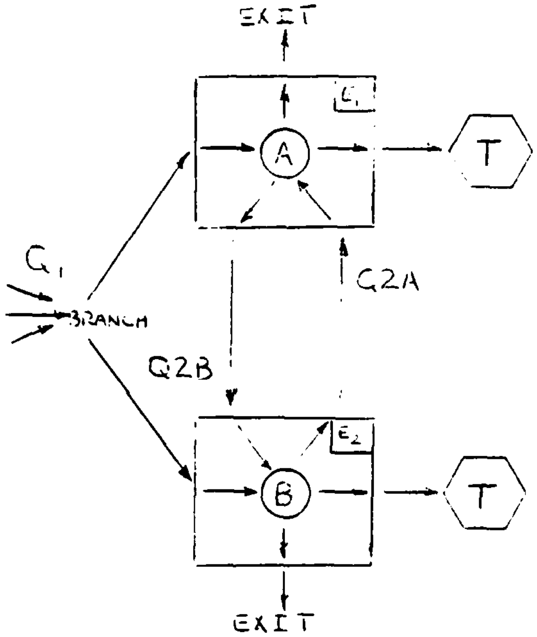


FIG B 2 1

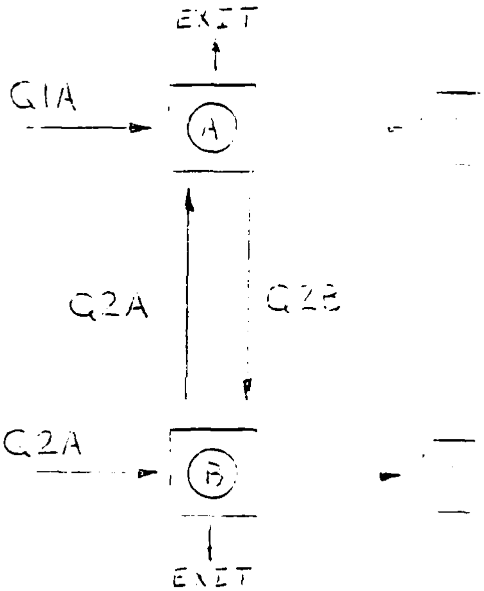


FIG B 2 2

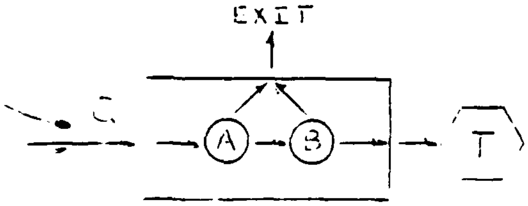


FIG C 1 1

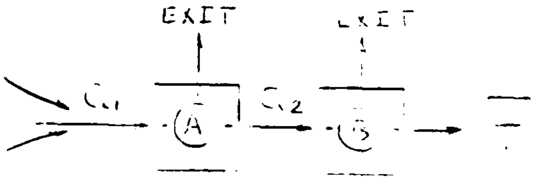


FIG C 2 1

BIBLIOGRAPHY

(1) Fejfar, A., "Test Results - Advanced Development Models of BISS Identity Verification Equipment, Volume I," MTR-3442, Vol I, 26 May 1977.

(2) Nycum, S., "Profiles of Computer Criminals," Proceedings of the First Annual Symposium, The Role of Behavorial Science in Physical Security, NBS Special Publication 480-24, 29-30 April 1976.

(3) Woodard,J. and Maier, J., "Automatic Entry Control for Military Applications," Proceedings of the 1979 Carnahan Conference on Crime Countermeasures, University of Kentucky, Lexington KY, 16-18 May 1979.

(4) Doddington, G., "Speaker Verification for Entry Control," Proceedings, Wescon Electronic Show and Convention, San Francisco, CA., 16-19 September 1975.

(5) Forsen, G., Nelson, M., and Staron, R., "Personal Attributes Authentation Techniques," RADR-TR-77-333, October 1977.

(6) Fejfar, A., and Benson, P. "Test Results, Advanced Development Models of BISS Identity Verification Equipment, Volume V," ESD-TR-78-150 Vol V, July 1978.

(7) Rehm, B., "Physical Access Control Using Automatic Speaker Verification," Proceedings of the 5th Annual IEEE Regional Conference, San Antonio, TX., 20-24 April 1980.

(8) Fejfar, A., "Combining Techniques to Improve Security in Automated Entry Control," Proceedings 1978 Carnahan Conference on Crime Countermeasures, University of Kentucky, Lexington, KY, 17-19 May 1978.

James R. Clifton
and
Lawrence I. Knab

Center for Building Technology
National Engineering Laboratory
National Bureau of Standards
Washington, D.C. 20234

IMPACT RESISTANCE OF CONCRETE

1. INTRODUCTION

The materials used in constructing security barriers and protective structures have not changed significantly over the past 30 years. Many of the present practices are based on the Corps of Engineers Manual "Fundamentals of Protective Design" published in 1946 [1]. While this manual remains as the authoritative source in the open literature, improvements and changes in the types and properties of structural materials have been made since 1946. The need to improve the penetration resistance of security barriers was clearly demonstrated by Moore [2]. He showed that man-passable openings could be developed in typical security barriers in relativelv short times using readily obtainable portable tools and explosives. In many instances, these openings could be produced so quickly that a reappraisal of the use of these barriers for physical security applications was required. In general, only concrete materials gave worthwhile resistances, but even some of them could be breached in an unacceptably short time.

The National Bureau of Standards (NBS) is carrying out a project to develop a technical basis for selecting materials which can be used in constructing barriers with improved penetration resistance. An important part of this work is the development of performance tests which can be used to evaluate and compare the penetration resistances of structural materials. In the past most security barriers have been constructed using concrete, and concrete will undoubtedly be specified in most future constructions of security barriers. However, in a recent review [3] of the penetration resistance of concrete, it was noted that performance tests are needed to determine the penetration resistance of concrete. The first phase of the NBS project, therefore, is concerned with developing appropriate performance tests for concrete. Tests being developed to measure the impact resistance of concrete specimens are described in this report and some test results are presented.

2. IMPACT TESTS

Performance tests are currently being developed to determine the resistance of concrete to single impact, repeated impact, and to small arms and small projectiles. It is intended to develop performance tests which can be readily performed safely within an enclosed laboratory and which can provide a basis for comparing the penetration resistances of different concretes. After developing the needed performance tests, minimal acceptable performance levels, i.e. performance criteria, will be proposed.

2.1 SINGLE IMPACT TEST

To determine the resistance of concrete to a single impact, a falling weight impact apparatus with a high mass impactor was constructed (Fig. 1A). The impactor weighs 300 lb (136 kg) and has a impacting diameter of 8 in (203 mm). It can be dropped from heights up to 10 ft (3 m). A 5 ft (1.5 m) drop has been found to be sufficient to cause shear failure in all the concrete specimens tested to date. Concrete beams, 3 x 3 x 15 in (76 x 76 x 381 mm), are clamped at both ends and impact occurs in the 8 in (203 mm) middle span.

The velocity of the impactor immediately before and after it strikes a concrete beam is measured. The energy required to fracture the concrete can be calculated from:

$$\text{Fracture energy} = (1/2)M\ (V_1^2 - V_2^2)$$

where M is the mass of the impactor and V_1 and V_2 are the velocities of the impactor before and after impact, respectively.

2.2 REPEATED IMPACT TEST

The resistance of concrete to repeated impacts, e.g. from a sledgehammer, is being determined using the apparatus shown in the right side of Figure 1B. The impact hammer weighs 11 lb (5 kg), has a diameter of 2.4 in (61 mm), and is 9 in (229 mm) long. Its striking face has a geometrical shape similar to the head of a common sledgehammer. The hammer is dropped from a height of 6 ft (1.8 m) and strikes the central region of a concrete slab. The hammer is dropped repeatedly until failure occurs as noted by the appearance of a perforation extending through the concrete slab. Concrete test slabs are 2 x 2 ft (610 x 610 mm) and 3 in (76 mm) thick. A square steel frame with a 1 in (25 mm) wide ledge provides support for the outer edges of the slab.

Dynamic cracking processes in concrete subjected to impact largely control its resistance to impact. However, these processes have been relatively unexplored. For the purpose of identifying the concrete design variables (i.e., mix proportions, and reinforcement), that have the largest influence on the resistance of concrete to repeated impact, the depth of penetration by the impact hammer is being measured during the course of each test. In addition, a measure of the extent of cracking is obtained by measuring the ultrasonic pulse velocity of concrete across the impact region. An 11 lb (5 kg) cylindrical projectible, with a hemispherical head (1.25 in (32 mm) radius), is used for tests involving depth of penetration and ultrasonic pulse measurements. Relationships are being sought between the depth of penetration and extent of cracking, as a function of the number of impacts for different concrete design variables.

2.3 PROBE PENETRATION TEST

The resistance of concrete to small arms or small projectiles is usually difficult to test in most laboratories. NBS is exploring the feasibility of adapting a standard nondestructive test method (Test for Penetration Resistance of Concrete, ASTM Designation C 803 [4]) used for predicting the strength of concrete by firing a probe into it. The probe is fired into the concrete with a 38 caliber charge (Fig. 1C) and the depth of penetration, crater volume produced on the firing side, and scab volume (crater produced on side opposite the firing side, see Fig. 1D) are measured. Concrete test specimens are 2 x 2 ft (610 x 610 mm) and 3 in (76 mm) thick.

3. TYPES OF CONCRETE BEING EVALUATED

Types of concrete which appeared to be promising materials for constructing security barriers were identified in the review by Clifton [3]. These included:

(1) concrete reinforced with steel reinforcing bars,

(2) concrete reinforced with expanded metal,

(3) concrete reinforced with discrete steel fibers,

(4) latex modified concrete,

(5) latex-modified fiber-reinforced concrete,

(6) polymer impregnated concrete and

(7) polymer concrete.

Concretes (1) through (5) can be prepared and placed by conventional construction equipment and practices whereas concretes (6) and (7) require special equipment and practices. During FY 80, the impact resistances of concretes (1) through (5) are being evaluated. The concrete mix design (i.e. amount of cement, water, and fine and coarse aggregate, see Table 1) for all the concretes is similar to that of concrete typically used in constructing security barriers. It has a nominal compressive strength of 5×10^3 PSI (34 MN/M^2) at 28 days.

4. RESULTS OF REPEATED IMPACT TEST

Results of repeated impact testing on the concretes tested to date are given in Table 1. The values obtained clearly demonstrate that the repeated impact test differentiates the penetration resistance of the concretes. In addition, this test appears to be reliable and is easily performed. The results indicate that steel fibers can substantially increase the impact resistance of concrete. The results with the 2 in (51 mm) long steel fibers are especially encouraging. A single layer of the expanded metal sheet also increased the impact resistance as compared to the steel reinforcing bar but was far less effective than the steel fibers.

Preliminary results using ultrasonic pulse velocity methods to detect crack development and propagation are presented in Figure 2. Relationships between the depth of penetration by the impactor and the reduction in ultrasonic pulse velocity as a function of the number of impacts are shown. Work is in progress aimed at seeking relationships between depth of penetration, crack propagation, and reduction in ultrasonic pulse velocity as a function of the number of impacts.

5. SUMMARY

A technical basis is being developed for selecting materials which can be used in constructing security barriers with improved penetration resistance. The first phase of the work is concerned with developing rational performance tests for evaluating the impact resistance of concrete. Three impact tests are currently being developed to determine the resistance of concrete to single impact, repeated impact, and to small arms and small projectiles. After the performance tests are developed, performance criteria will be proposed.

Preliminary results from repeated impact tests indicate that steel fibers can substantially increase the impact resistance of concrete as compared to expanded metal and conventional steel bar reinforcing. Ultrasonic pulse velocity measurements appear to be useful in assessing the crack damage occurring during the repeated impact test.

6. ACKNOWLEDGMENT

Support of this work by the Defence Nuclear Agency is gratefully acknowledged. The authors express their gratitude to Dr. David Jenkins, University of Central Florida, for many helpful suggestions and stimulating discussions.

7. REFERENCES

1. Fundamentals of Protective Design, Engineer Manual fcr War Department Construction (U.S. Corps of Engineers, 1946).

2. R. T. Moore, Barrier Penetration Tests, NBS Technical Note 837 (National Bureau of Standards, 1974).

3. J. R. Clifton, Penetration Resistance of Concrete - A Review, NBS Special Publication, In Press.

4. American Society for Testing and Materials (ASTM) "Tentative Test Method for Penetration Resistance of Hardened Concrete," ASTM C 803-75T, Annual Book of ASTM Standards, Part 14, Philadelphia, PA, 1978.

Table 1. Results of Repeated Impact Tests on Concrete[1] Slabs

Concrete Reinforcement	Number of Impacts to Failure[2]
No. 4 deformed steel bars on 12 in (305 mm) grid Steel reinforcing bars are located outside impact region and are centered about the midpoint of the thickness of the slabs.	10
1.3 in (33 mm) steel fibers[3] with hooked ends, 1 percent by volume based on concrete: No. 4 bar grid	51
2 in (51 mm) steel fibers with hooked ends, 1 percent by volume: No. 4 bar grid	126
0.25 in (6.4 mm) thick expanded metal, with hexagonal openings 1.5 x 3.5 in (38 x 89 mm). Expanded metal placed at midpoint of slab thickness.	19

[1] Concrete mix proportions by mass, based on cement: cement, 1; water 0.6; sand, 2.5; crushed limestone, 1.8. Concrete tested at 28 days.

[2] Failure defined as formation of perforation which is visually apparent.

[3] Fibers with hooked ends glued together side by side in bundles with a water soluble adhesive.

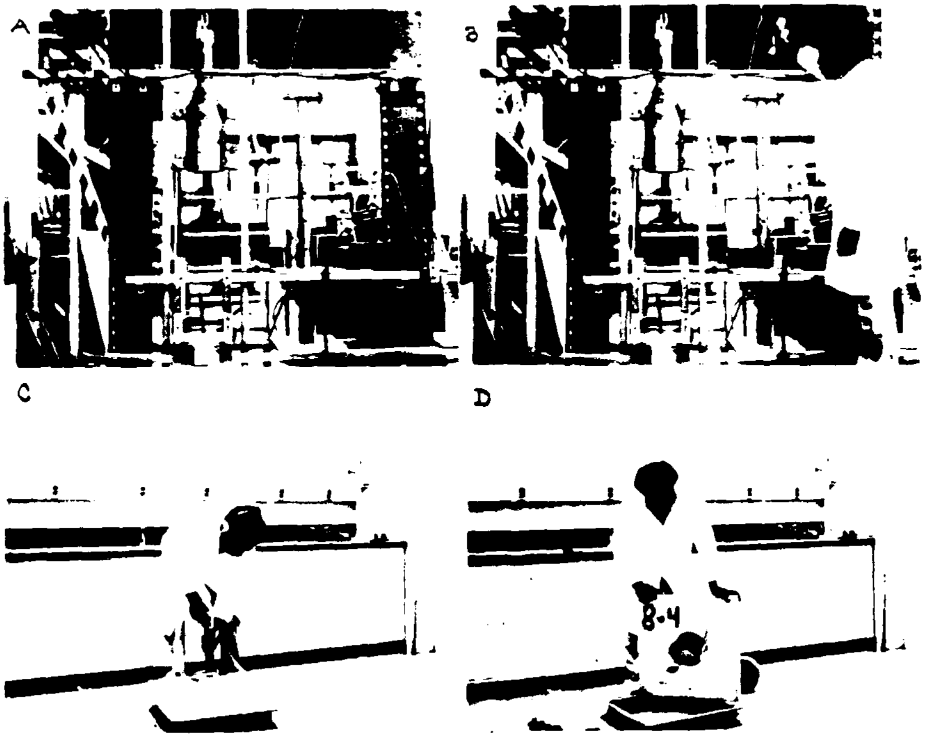


Figure 1. Impact Test.

A. Single impact tester with a 300 lb (136 kg) impactor. B. Repeated impact test using 11 lb (5 kg) impactor. C. Percussion probe test. D. Resulting scab from probe test.

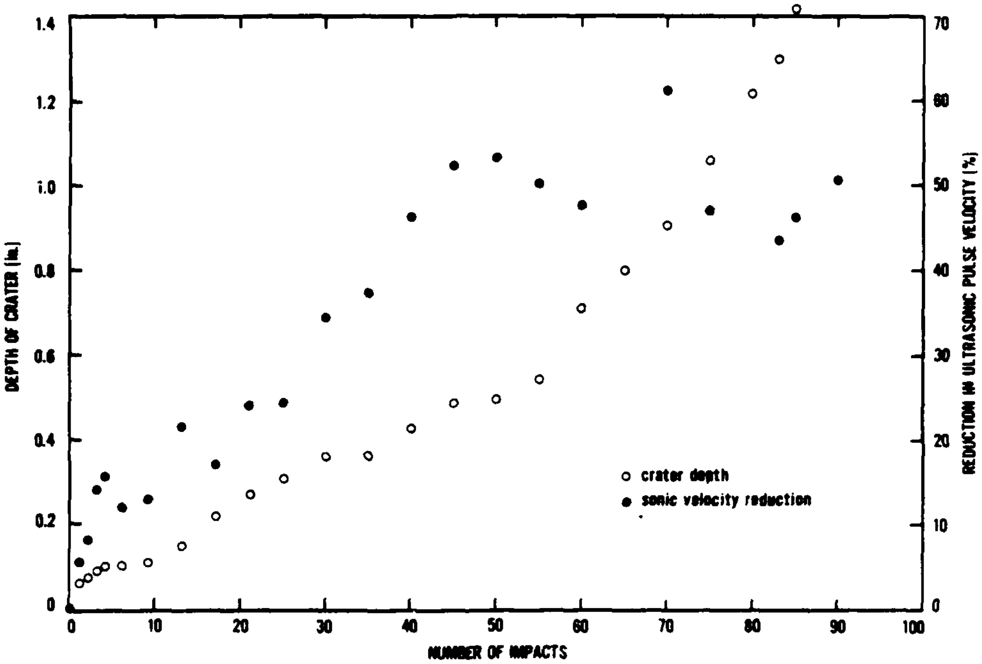


Figure 2. Ultrasonic Pulse Velocity and Depth of Crater results of Repeated Impacts. The impactor, which had a hemispherical head and weighed 11 lbs (5 kg), was dropped from height of 6 ft (1.8 m) on 3 in (76 mm) thick concrete slab containing 2 in (51 mm) long steel fibers with hooked ends (1 in = 25.4 mm).

AREA COVERAGE INTRUSION DETECTION SYSTEMS RESEARCH

by Larry Blankenship, JAYCOR, Inc.
June 10, 1980

Area or "volumetric" coverage by an outdoor intrusion detection system refers to the capability of that system to provide information on the position and movement of an intruder or intruders within a defined perimeter. Such position and movement information can be used to effectively direct forces to intercept intruders and/or to initiate action based on the depth of intruder penetration (e.g. emergency destruct or disable).

JAYCOR is presently performing research for DNA to determine the feasibility and practicality of modifying microwave IDS technology to accomplish area coverage. As this research effort is in its early stages, this report will outline the approaches under investigation, identify some potential technical problem areas, and briefly raise some of the operational and behavioral science questions which might arise should such a system be deployed.

Microwave IDS technology is being investigated for this application because of several potential advantages:

1. The detection paths are clear of any physical structures thus allowing free movement through the area by authorized personnel.

2. The lack of a requirement to erect structures or bury cables along the detection path make microwave IDS technology potentially very cost effective.

3. The frequency of operation (10.525 GHz) is relatively insensitive to changes in weather.

4. Because of the physics of the propagation phenomenon some volume coverage is obtained in each microwave beam, reaching a maximum at the midpoint between transmitting and receiving antennas.

Commercially available microwave IDS units designed for perimeter use have several disadvantages which must be overcome, however. These are primarily their susceptibility to nuisance alarms and the manufacturers' requirements that terrain between the transmitters and receivers be graded to a high degree of flatness.

JAYCOR's approach to determine if such a microwave area coverage system is practical and feasible can be described in six phases, many of which are concurrent and interdependent. Each of these six phases will be discussed below and the present status of work in that phase indicated.

Phase 1: Examine existing commercial units.

Existing commercial microwave IDS systems were examined for their potential adaptability to the testing requirements of this program. After an initial paper study, two units were purchased and tested. Those units were the Shorrock

Model 33 and the Racon Model 14000. While both units functioned per manufacturers' claims, the Racon was found to be much more readily adaptable and is therefore being modified for use in the testing phases of this program.

Phase 2: Build a system for data collection, modification, testing, and evaluation.

The design for the test system is approximately 95 percent complete at this point, construction is underway, and initial testing will begin this month.

The design of a test system must address the questions of area coverage grid patterns. The most straightforward approach to an area coverage grid is the use of transmitter-receiver pairs dedicated to one another and arranged in a crosshatch matrix as shown in Figure 1. This simple approach has the advantage of dividing the area into rectangular sectors which may be called out in an XY coordinate manner thus allowing easy position identification of an intruder. This configuration does not, however, allow for the economic gains which might be achieved by using one transmitter to drive multiple receivers. Additionally, it does not allow for a "clear zone in the center at which the valuable resoures rest. Such a clear area may or may not be desirable depending upon the particular resource and installation.

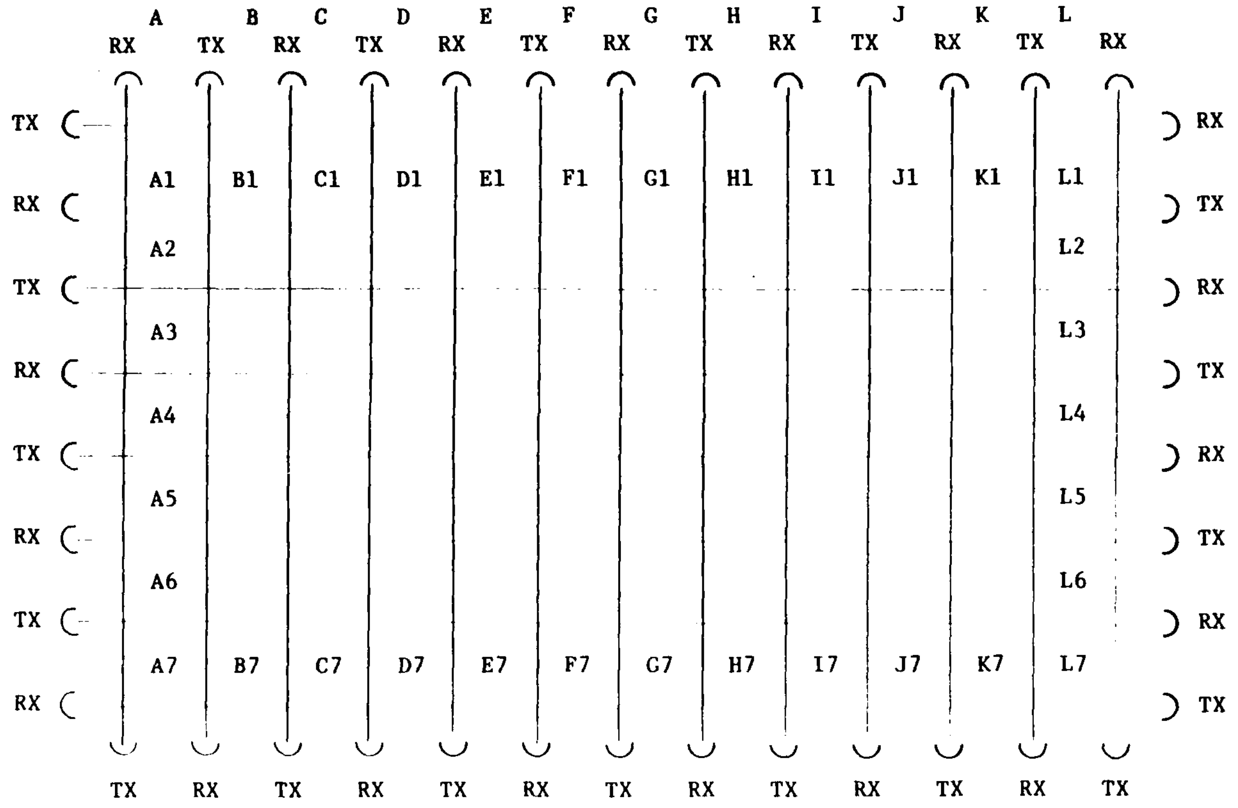
The initial test field will take into account these latter considerations by employing three receivers per transmitter in a pattern which can allow a center clear area if desired. The test field pattern as it is being implemented is shown in Figure 2. This particular pattern can provide perimeter coverage (which may be augmented by other perimeter IDS) as well as depth of penetration information. Each section of the covered area consists of two transmitters and six receivers in overlapping patterns as shown. If four such patterns are placed at ninety degree angles and joined at the corners, a square area is covered with a clear center as shown in Figure 3. This concept is not limited to square areas nor is it limited to three receivers per transmitter. An irregular six-sided area is also shown in Figure 3 with one possible pattern. If the concept proves to be practical, the pattern variations available to adapt to the needs of a particular installation are numerous.

The hardware implementation of the test system is shown in block diagram form in Figure 4. Each of the receivers is capable of detecting only one, unique modulation frequency. By varying the modulation frequency on each of the transmitters, an electronic scanning can thereby be obtained. The rapid series of changing modulation tones allows for a continuous system integrity check. In sequence, the system controller must tell the transmitter to change its modulation frequency, the specific receive unit with that modulation frequency must respond, and the response be noted back at the system controller. This insures the entire loop is functioning and is repeated many times per second.

The essence of the data collection process is the Tektronix 4052 system controller/graphics computer. The intruder signal wave forms are digitized and placed both in the 4052 memory bank and on magnetic tape. Analysis of the signals may be performed both immediately and/or repeated at a later date.

SIMPLE CROSS HATCH GRID PATTERN

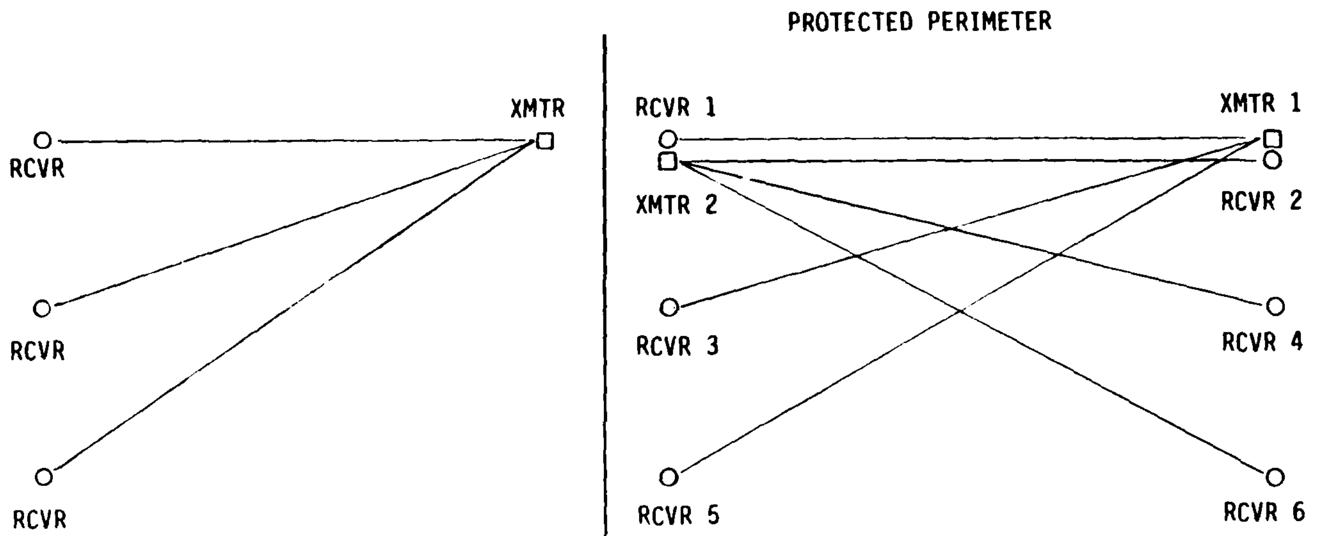
- Can provide orderly sectors if real world conditions permit.
- Does not take advantage of each transmitter's capability to drive multiple receivers.



A
B
C
D
E
F
G
H
I
J
K
L
RX TX RX TX RX TX RX TX RX TX RX TX RX
TX
RX
TX
RX
TX
RX
TX
RX
A1 B1 C1 D1 E1 F1 G1 H1 I1 J1 K1 L1
A2
L2
A3
L3
A4
L4
A5
L5
A6
L6
A7 B7 C7 D7 E7 F7 G7 H7 I7 J7 K7 L7
RX
TX
RX
TX
RX
TX
RX
TX
TX RX TX RX TX RX TX RX TX RX TX RX TX

FIGURE 1

TEST FIELD PATTERN



ONE COVERAGE "GROUP" CONSISTS OF ONE TRANSMITTER AND THREE SPACED RECEIVERS. EACH RECEIVER HAS A UNIQUE FREQUENCY TONE DECODER. THE GROUP IS SCANNED BY ALTERNATING THE TRANSMITTER MODULATION FREQUENCY BETWEEN THE THRFE RECEIVER TONES.

THE TEST FIELD WILL CONSIST OF TWO OVERLAPPING GROUPS:

ODD GROUP = XMTR 1 AND RCVRS 1, 3, 5

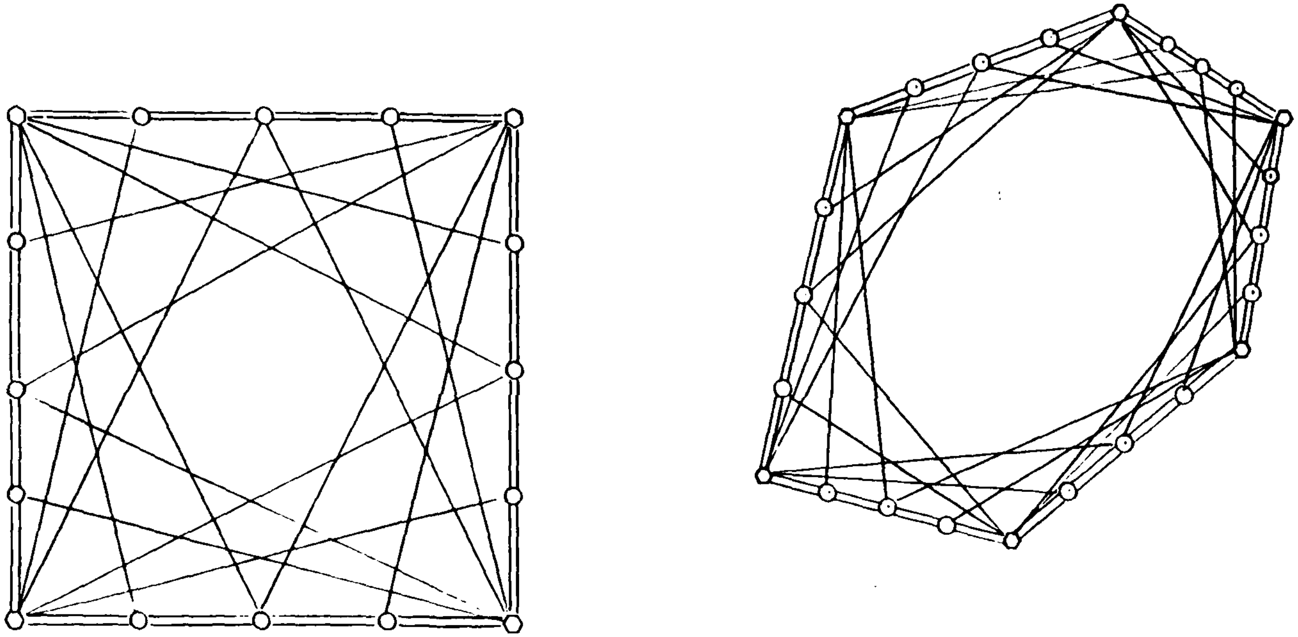
EVEN GROUP = XMTR 2 AND RCVRS 2, 4, 6

EACH GROUP SCANS INDEPENDENTLY AND HAS INDEPENDENT CIRCUITS FOR ACQUIRING AND DIGITIZING THE INTRUDER SIGNAL.

FIGURE 2

FIELD PATTERN EXTRAPOLATION

EACH EXAMPLE PROVIDES DUAL BEAM PERIMETER
COVERAGE PLUS DEPTH COVERAGE



IF THE TEST FIELD PATTERN IS DUPLICATED FOUR TIMES AT 90° INTERVALS, A SQUARE AREA IS PROTECTED.

THE PERIMETER COVERAGE GROUP PAIR CONCEPT WORKS EOUALLY WELL FOR IRREGULARLY SHAPED AREAS. THE RECEIVERS ARE SHOWN HERE AT EQUAL SPACING. RECEIVER SPACING AND THE NUMBER OF RECEIVERS PER GROUP CAN BE MODIFIED TO ADJUST THE DEPTH COVERAGE PATTERN IF DESIRED.

FIGURE 3

BLOCK DIAGRAM OF SYSTEM DESIGN

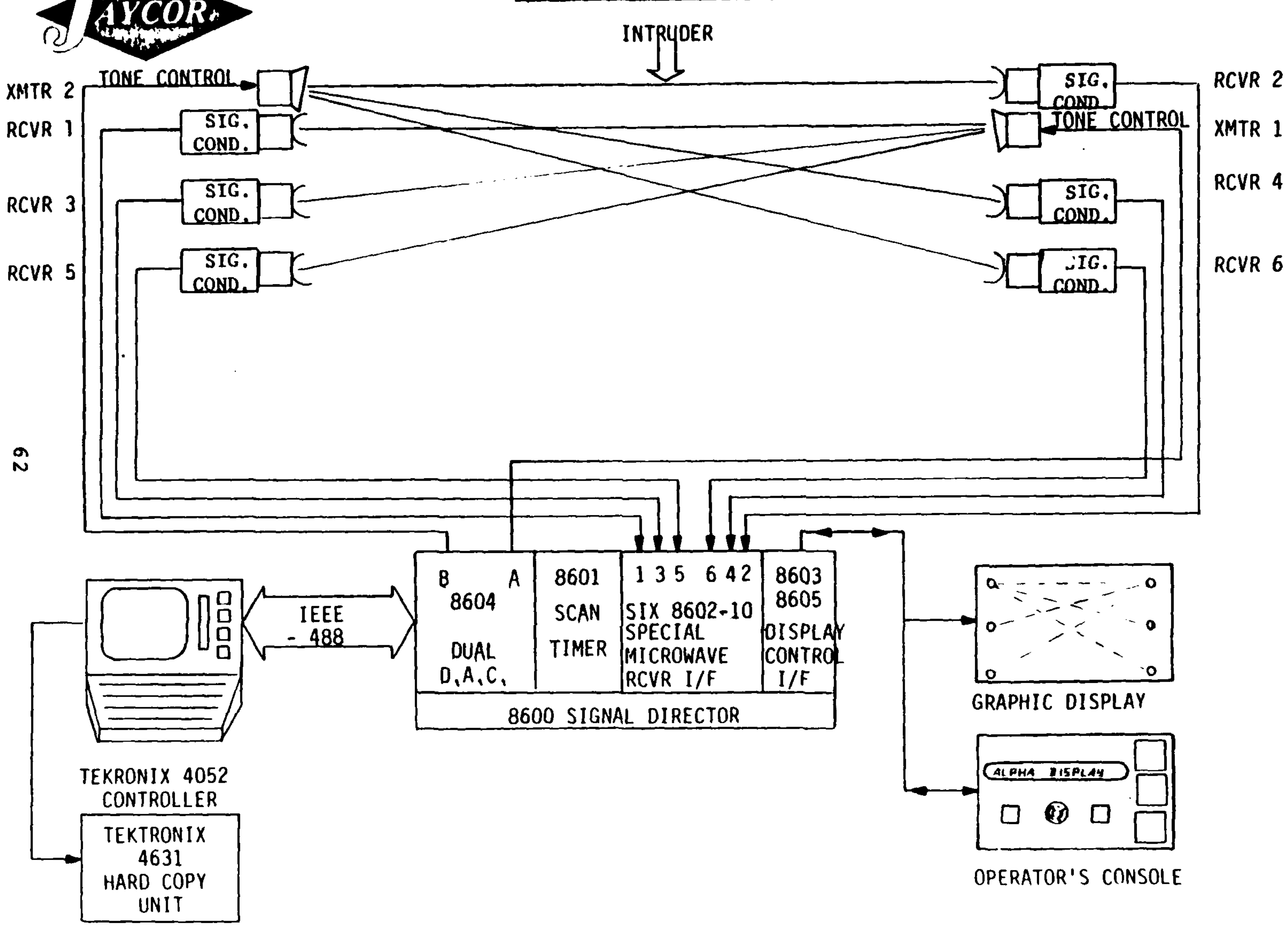


FIGURE 4

Phase 3: Simulated intruder testing.

Initially, testing will be done with single human intruders in an attempt to verify the level of performance of the data collection system, signal digitization techniques, and microwave scan methods. As the level of sophistication increases in the analysis software, more and increasingly difficult nuisance alarm situations will be introduced as well as intruder detection evasion techniques.

Phase 4: Signal analysis and nuisance alarm rate reduction.

Presently available commercial units employ simple techniques for intruder detection which provide little or no nuisance signal rejection. These units will go into alarm whenever their signal threshhold level is exceeded no matter what the characteristics of the signal itself. By introducing signal processing into the system, it is anticipated that a reduction in the nuisance alarm rate may be achieved. Initially nuisance alarm discrimination tests will be performed with a wide variation between the intruder and the nuisance alarm signals. For example, the difference between a human walking at a normal pace through the covered area as opposed to items such as leaves blowing through the area or birds flying through the area. As key characteristics between these signals are differentiated and algorithms implemented to discriminate between them, tougher discrimination tasks will be tested such as the differentiation between a human crawling with his shoulders perpendicular to the microwave so as to present minimum radar cross section and a small animal such as a rabbit within the field. The level to which such discrimination can be taken has yet to be determined. The objective at this point is to reduce the nuisance alarm rate to a more acceptable level. Much work has been done in other IDS to quantify an intruder's "signature". Whether or not such sophisticated signal processing is achievable or even desirable for an area coverage IDS has yet to be determined. Once algorighms are developed for nuisance alarm reduction, they will be implemented through a combination of hardware discriminators and/or software programming.

Phase 5: Microwave field terrain sensitivity analysis.

Commercial microwave IDS units claim long usable ranges (1500 feet) using very low transmitter power (5 milliwatts). Commercial manufacturers also require that the terrain between the transmit and receive antennas be flat to within a few inches over this entire range. An analysis of the commercial units shows that such a range is only obtainable if the specular reflection patterns from a flat ground surface can be relied upon. Additionally, the commercial units must assume the use of their own fixed beam pattern antennas at both the transmit and receive points. While severe terrain variations such as sharp gullies or ridges cannot be tolerated, it appears that significantly less restrictive terrain specifications can be tolerated with improved signal path characteristics. Such improved signal path characteristics can be obtained by any combination of shortening the distances between transmit and receive antennas, increasing the receiver sensitivity, increasing the transmitter power, or modifying the antenna beam patterns so as to concentrate the signal. Analysis by computer modeling is presently underway to determine the extent of terrain variation or obstacles within the path which can be tolerated with varying beam shapes and power levels. In a deployable system, a series of options may be desirable. A broad coverage antenna selection for very flat terrain and narrower beam antenna selections for rougher terrain. An experimental antenna is presently being developed which will electronically select beam direction and shape. Such an antenna will be valuable in the testing process and may prove to be a key factor in cost effective deployable systems over varying installation characteristics. While such an antenna would not replace all fixed beam shape types, in many cases it might provide the means to optimize the area coverage system for a particular installation by means of a custom software site descriptor.

Commercial units utilize automatic gain control on the receivers only. This is a standard technique deployed in any radio network where the receivers are isolated from the transmit circuit. A disadvantage with this type of automatic gain control is that increasing gain to gather more signal also increases amplification of the background noise. In the area coverage system, both the transmitter and receiver will be in communication with a common point. Automatic gain control may then be accomplished by increasing transmitter power and/or receiver gain to obtain optimal signal-to-noise ratio characteristics. Each of the techniques described improves the signal transfer characteristics along the detection path and thus tends to decrease sensitivity to normal terrain variation. The extent to which these techniques can be employed in a practical system will be determined both analytically and experimentally.

Phase 6: Operational system considerations.

If the results of the various stages of analysis and testing described in phases one through five so indicate, it will be undertaken to determine and recommend a practical approach for operational implementation of an area coverage IDS. While this phase certainly has many technical questions to be answered (central versus distributed processing, programmable versus fixed antenna selections, maximum transmit power levels, anti-vulnerability features, price/performance tradeoffs, etc.), the behavioral science questions raised in the man-machine interfacing of such a system become much more philosophically interesting. Many of the questions raised in man-machine interfacing and operator confidence level are common to any such sophisticated system. There are, however, some unique situations presented by an operational area coverage system which present challenges to procedure as well as equipment design. Some of the questions that must be addressed during this phase are listed below.

o How can a large number of sensor paths be displayed to the operator in a non-confusing yet non-limiting manner?

o In what manner should intruder position and movement information be displayed?

o What type of operator feedback to acknowledge an intruder position can be implemented to allow ease of acknowledgment and still provide positive indication of understanding (flashing graphic touch panel methods have been suggested)?

o What clear communication protocol can be established for the IDS operator to direct response forces to intercept intruders whose movements and multiplicity are displayed?

o Should some "identification friend or foe" system be employed which would display response forces as well as intruder forces and what are the technical and cost impacts of such a decision?

o Previous systems have displayed an alarm or no alarm. The envisioned system will detect a disturbance and perform an analysis as to the probability of a valid intrusion. What display, if any, should be employed for this "grey area" during analysis?

o What design features can be included to maximize operator confidence in the system (e.g. self-test features)?

o If possible, would it be desirable to eliminate 100 percent of nuisance alarms or is it more desirable to have a small number of such random alarms?

o To what level can or should the area coverage system man-machine interface be integrated with the other detection systems at any given installation?

The research effort into area coverage techniques is clearly still in the technical phases. The questions raised above regarding man-machine interface and behavioral science aspects of such a system will be addressed as technical implementation of the system proves to be practical.

THE POTENTIAL OF OLFACTORY RECEPTION FOR ULTRATRACE CHEMICAL ANALYSIS

R. B. Murphy
Department of Chemistry, New York University
New York, NY

There is much precedence for the idea of simulating man's senses by artificial means and the olfactory sensing process has fascinated many scientists. In recent times numerous attempts have been carried out at linking computer based measurement systems with individual sensory neurons, but none have been sufficiently reproducible to possess any real analytical utility.

Natural senses have many advantages over even the best synthetic detection systems, particularly with regard to selectivity and in many cases sensitivity. The mechanism of discrimination of different odorants by the nose is a matter of some debate. Obviously the process takes place at a conformationally sensitive receptor site located in the nerve cell membrane. Based on our knowledge of other types of biological receptors, such as those which interact with acetylcholine, insulin, and certain steroid hormones, it is clear that the action to the site depends on a specific protein which is capable of binding the olfactant. A structural reassociation occurs in the biological macromolecule upon binding, which results in a perturbation in the active ion transport of the cell. The ionic flux imbalance gives rise to the observed electrical activity.

For some time, our group has been principally interested in molecular studies of receptor biochemistry. Our approaches have included photoaffinity labeling in the dopamine neuroreceptor [1][1], the design and application of receptor specific fluorescence probes in the beta-adrenegric reporter system [2,3], and the interrelation of ion transport to specific receptor systems [4,5]. In the area of olfaction, the nature of the "receptor" or receptors for chemosensory information is not so well defined from a biochemical point of view. Consequently, a major portion of our efforts have been directed toward the biochemical elucidation of the structure and function of olfactory chemoreceptors. Although a considerable number of studies have been attempted in this general area [6-10], virtually nothing is known with certainty as to the biochemistry of mammalian olfaction.

[1] Numbers in brackets refer to the references at the end of this paper.

The research program on olfactory reception includes three main studies. The first is to isolate the proteins and measure their activity for detecting odors, the second is to determine as much as possible about the biophysics of the *in vivo* olfactory process and the third is to use the information obtained from the above studies in an attempt to simulate the olfactory process in an artificial system that can be used as a quantitative analytical instrument.

Clearly the benefits to be derived from such a device are significant if one can develop a device that approximates the olfactory sensing capability of the biological entity. Although accurate data are unavailable, estimates of insect sensitivity to a pheremone approximate a few molecules per square centimeter. The detection limit for a trained dog detecting explosive residues appears to be in the picomolar per square centimeter region.

THE BIOCHEMISTRY OF OLFACTORY DETECTION

The basic approach is to separate as pure a fraction of protein as possible from the olfactory epithelium of the rat and to reconstitute this material on a phosphatidylcholine bilayer. The properties of the bilayer are then examined in a number of ways as described in the next section.

Recent work by Cagan [11] has given strong support to the concept that the olfactory reception proteins are in the cilia or the epithelium. Therefore, our work has concentrated on separating the cilia from the underlying substrate cells. The separation techniques which utilize sonication for 1 min at 4°C and gel filtration on Sephadex G-200 indicate the presence of protein associated with the cilia.

Another series of studies have been made on the binding of an odorant to two main whole homogenates, one, from the olfactory epithelium and the other from respiratory epithelium. Sulfur-35 labeled diethyl sulfide is used in two methods of measurement; the standard filter binding assay method of Seeman et al. [12] and a centrifuge technique which produces a low background. The results of these experiments show that specific binding of diethyl sulfide to the homogenates of the olfactory epithelium can be verified at the micromolar level. Our current understanding of the olfactory process indicates that binding at the nanomolar level should occur. Additional experiments to verify this fact are in progress.

Another technique developed in this laboratory is to measure the binding of a luminescent odorant. Here, exceptional sensitivity can be realized via photon counting of the luminescent radiation. Using 2 ethoxynapthalene one can observe a high affinity binding site with a K_D approximating 8 nM. These preliminary data show great promise as a new method for the determination of affinities of olfactory epithelium for odorants.

THE BIOPHYSICS OF OLFACTORY DETECTION

Artificial bilayer membranes are prepared from cholesterol, n-decane and phosphatidylcholine. These layers are mounted in a chamber shown in figure 1. The chamber is totally enclosed on the right side. Attached to the right side is a piston operated by a stepping motor This feature in conjunction with the attached electrodes allows the computer-controlled system to measure automatically the current-voltage parameters, ac capacitance and surface tension of the membrane.

The results of studies are typified by an experiment which was carried out with relatively crude phosphatidylcholines. Other experiments using components of higher purity for the bilayer preparation are in progress. The temperature was maintained within ±0.05°C. The notations "OL" and "ET_2S," refer respectively to the sequential addition of an olfactory homogenate, and an odorant to the chamber. The olfactory homogenate was prepared as previously described in this report, and contained a Lowry protein concentration of 280 μg/ml. One hundred microliters of this solution was added to one side of the chamber. The odorant utilized was diethyl sulfide, added at

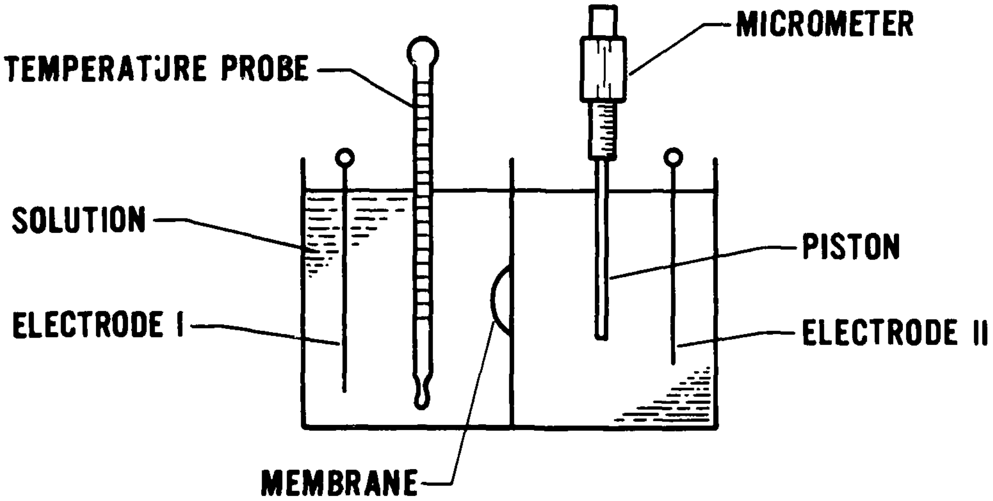


Figure 1. The bilayer chamber showing the principle of the surface tension measurement. A small piston is forced into one (closed) side of the chamber in order to maintain a constant area of the membrane.

a concentration of 100 μl of $2x10^{-6}$ molar solution. Not illustrated is the control experiment; the addition of the odorant to the system in the absence of the olfactory homogenate was without effect. Only at concentrations of odorant in the vicinity of 10^{-6} M did nonspecific interaction with the membrane introduce observable perturbation in ac and dc electrochemical properties.

It is seen from figure 2 that the ac and dc properties of the system appear to change somewhat differently with the two

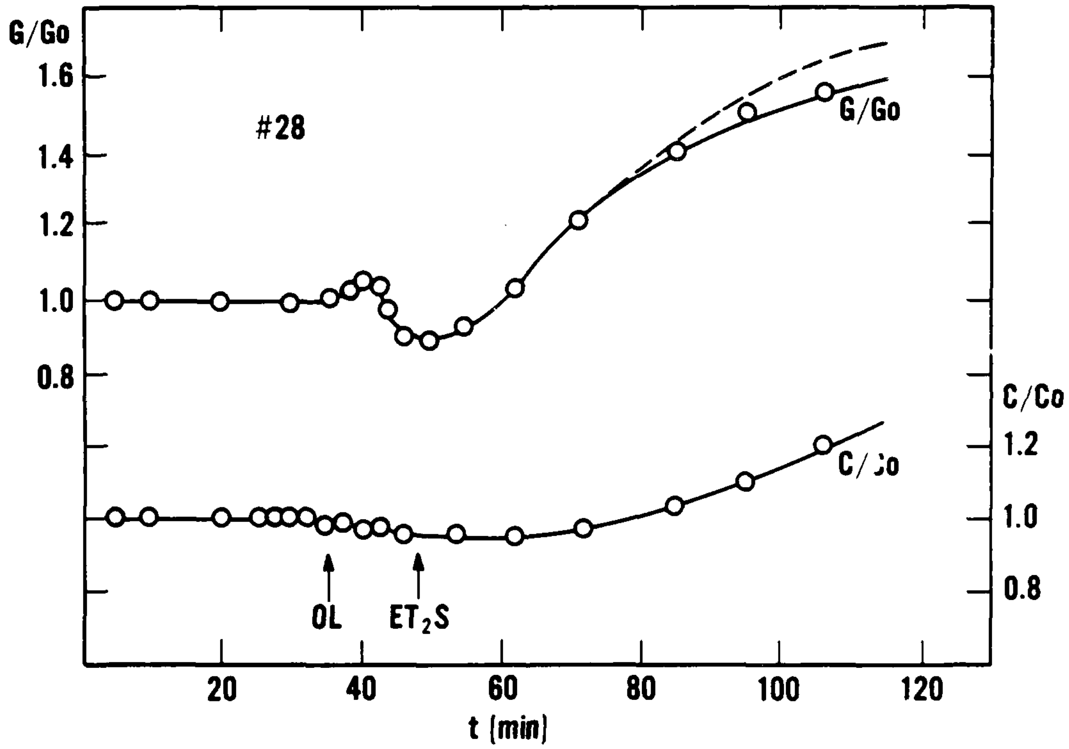


Figure 2. Time dependence of the relative conductivity and capacitance of bilayer membrane upon the asymmetric addition of olfactory homogenate and diethyl sulfide. Conductivity: solid line (corrected for change in capacitance). Bathing solutions: 50 mM Tris-Maleate, 1 mM Ascorbate, 7 mM NaCl, 7 mM KCl, pH adjusted to 7.40. Temperature +27°C+0.05°C. OL: Addition of olfactory homogenate (100 μl) containing 240 μg Lowry determinable protein per milliliter. ET_2S: Addition of 100 μl of ethyl sulfide $(2.0x10^{-6}$ m). Time from homogenate of epithelium to experiment: 1 d. $G_0 = (1.37\underline{+}0.05) \times 10^{-7} ohm^{-1} cm^{-2}$; $C_0 = (0.39+0.02)\ \mu F/cm^{-2}$.

additions, although the information appears to be complementary. The addition of the olfactory homogenate causes no change in capacitance, although a small transient increase in dc conductivity is observed. However, when the diethyl sulfide is added, a slow but irreversible increase in both the dc conductivity and the capacitance is observed. The most surprising fact is the extremely slow response.

An additional experiment using a slightly different type of bilayer produced results as shown in figure 3. We observe here

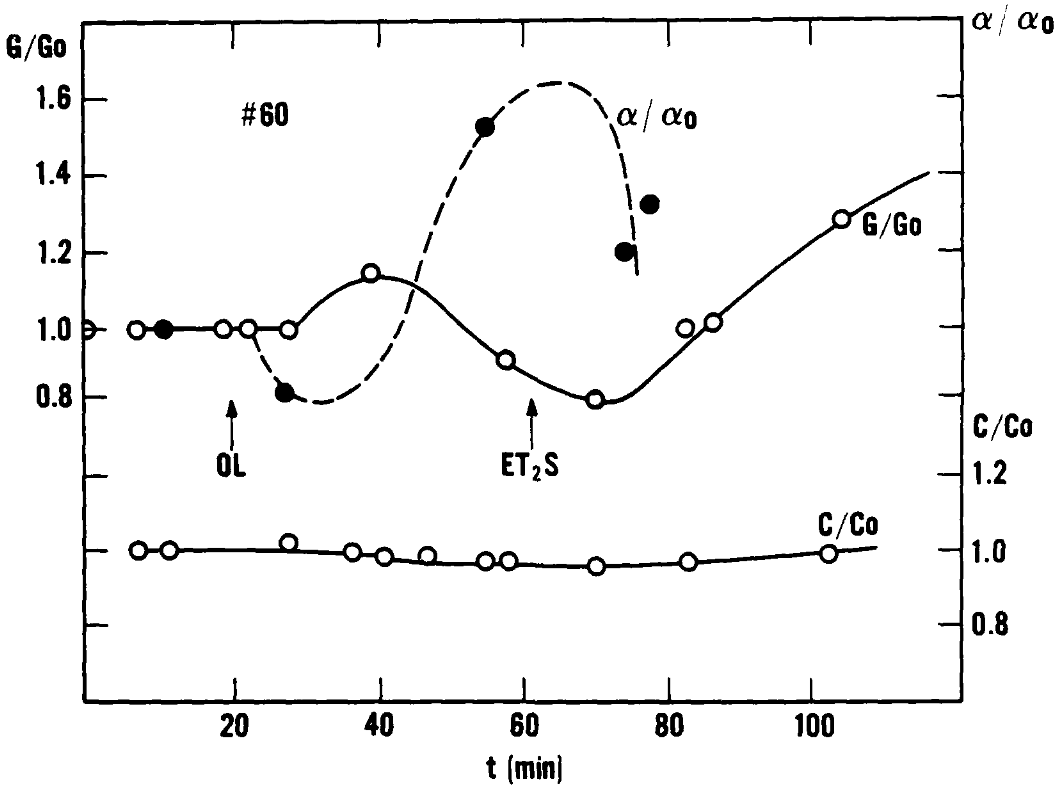


Figure 3. Time dependence of relative conductivity, capacitance, and surface tension of membrane on asymmetric addition of soluble fraction from sonicated olfactory homogenate, pelleted at 100,000xg., and diethyl sulfide. All conditions as above, except: buffer contains 20 mM NaCl and KCl, $G_0 = (8.85 \pm 0.05) \times 10^{-8}$ ohm^{-1}cm^{-2}; $C_0 = (0.41 \pm 0.02)$ μF/cm^{+2}; $\alpha_0 = 0.8 \pm 0.1$ dyn/cm. Protein concentration = 0.940 mg/mL.

a change in capacitance and dc conductivity almost identical to the previous experiment. Additionally, the surface tension of the membrane was measured as a function of time throughout this experiment. It is observed that the greatest perturbation induced in the experiment by the addition of odorant to the system is in the surface tension, and not in the capacitance or the dc conductivity. It is further striking in that an effect is evidenced albeit in the opposite direction simply upon the addition of the olfactory protein. Again, in other experiments it was shown that the odorant itself in the concentration regime in which it was applied was without effect on either the capacitance, dc conductivity, or surface tension of the system.

In order to examine the time course of the experiment, which could not be altered by changes in buffer composition (such as the addition of calcium ion or EGTA to the system), we decided to examine the possibility, that gramicidin might introduce a faster response because it is known to produce microscopic holes in the bilayer. The change in DC conductivity is far larger than that which was previously observed in these studies. However, the time course of the reaction is unaffected by this treatment.

PROSPECTS FOR A PRACTICAL OLFACTORY DEVICE

We have demonstrated that a protein fraction can be obtained from homogenates of the olfactory epithelium which will sensitize lipid bilayers to the specific action of certain odorants. We have further demonstrated that this effect which is not due to nonspecific interaction of odorant with the lipid membrane itself, occurs at extremely low odorant concentrations, and is specific to olfactory epithelium.

A number of major studies remain to be done. First, selectivity of the homogenate to a single odorant has not been evaluated. Second, reproducibility of the response of the homogenate needs to be improved. Third, a device which is to be deployed in the field must necessarily have a rapid response time. Fourth, the bilayer must be mechanically stable.

Major progress has been made in mechanical stability of the bilayer. The approach to preparation involves dipping of a Teflon plate into a monolayer. The Teflon plate is machined with one or more holes (diam. 0.2 mm), the anterior of each hole being sealed with cement and containing a small silver wire. If properly dipped into a monolayer, a lipid bilayer membrane which is completely solvent free can be formed. The chambers are closed, which means that provided the device is maintained in a proper aqueous medium it can be handled quite roughly, and the membrane will remain intact. We have made such a device with several holes, and have demonstrated that it responds in a normal manner to gramicidin, indicating that we have formed a lipid bilayer membrane in our apparatus. It is conceivable that such plates can be made with thousands of holes, each hole being a chamber.

SUMMARY

In summary we have demonstrated that the olfactory approach is potentially of considerable value as a quantitative analytical tool. We intend to concentrate on both the necessary biochemistry and biophysics to enable us to understand the genesis of the effect, while continuing to emphasize the novel bilayer approaches toward the construction of a practical device, with selectivity which can be tailored to the desired end use, with sufficient stability and minimum response time so that it will be functional in the field.

PEFERENCES

1. Murphy, R. B., Thermos, K., Huie, K., and Schuster, D. I., "Photoaffinity Labeling of a Solubilized Dopamine Neuroreceptor Preparation," Submitted to J. Biol. Chem.

2. Murphy, R. B., Cherksey, B., and Zadunaisky, J., "Propranolol as a Specific Probe of the Beta-Adrenergic Receptor in the Frog Erythrocyte," Anal. Biochem, in press.

3. Cherksey, B., Murphy, R. B., and Zadunaisky, "Cytoskeletal Linkage of the Propranolol Labeled Beta Adrenergic Receptor-Adenylate Cyclase Complex in the Frog Erythrocyte," Submitted to Proc. Nat. Acad. Sci. (U.S.A.).

3a. Cherksey, B., Ph.D. Thesis, "Propranolol as a Specific Probe of the Beta Adrenergic Receptor," New York University Department of Chemistry, 1980.

4. Murphy, R. B., "DIDS as a Specific Fluorescence Probe of the Erythrocyte Anion Transport System of the Human Erythrocyte," Submitted to Biochem. Biophys. Res. Comm.

5. "Murphy, R. B., "DIDS-Complex with the Erythrocyte Anion Transport System as a Probe of the Pressure Dependence of Anion Translocation in Ghost Cells," submitted to J. Membr. Biol.

6. Getchell, M. L., and Gesteland, R. C., (1972). Proc. Natl. Acad. Sci. (U.S.A.) 69 1494-8.

7. Menvese, A., Dodd, G., and Poynter, A. (1977). Biochem. Soc. Trans. 5, 191-194.

8. Cagan, R. H., and Krueger, J. M. (1976). J. Biol. Chem. 251, 88-97.

9. Cagan, R. H. (1980) in International Symposium on Olfaction and Taste: Biochem. Aspects (in press).

10. Dodd, G. (1980) Ibid.

11. Cagan, R. H., to be published.

12. Seeman, P., Proc. Nat. Acad. Sci. (U.S.A.) 72 4376 (1975).

QADDAFI HAS ONE OF OUR NUKES

OR

SOME THINGS WE NEED TO KNOW ABOUT BEHAVIORAL SCIENCE AND SECURITY

Donald R. Richards
Booz·Allen & Hamilton Inc.
4330 East West Highway
Bethesda, Maryland 20014

At a recent technology symposium, the keynote speaker said, "If we lose the battle for peace,..." The battle for peace is the effort to deter our adversaries from taking actions which will lead us into a conflagration. One of our major weapons in the battle for peace is our nuclear capability, both tactical and strategic. Loss of one of these parts of our deterrent strategy could have major negative impact on the balance of deterrence in the "battle for peace."

How could we lose one of these major elements? I think most of us would agree that if a major tragedy occurred at one of our nuclear weapons sites, either a plutonium-scatter or an accidental or purposeful nuclear detonation or even perhaps some individual or group taking one of our weapons hostage... any of these things would certainly produce major international publicity and media coverage and would certainly lead to strong efforts on the part of some people to demand withdrawal of these weapons from many locations. The ultimate effect could well be an impact on our tactical nuclear deterrence, a change in that precarious balance of power which many people believe keeps the world from dissolving into a nuclear fireball.

This symposium exists to bring behavioral science and security personnel together in order to better integrate the two fields in basic support of the security responsibility. The reason I am raising the issue of the nuclear deterrent is because of its critical importance and because it points up some areas in which behavioral tools are needed. A great deal of outstanding work has been done in the behavioral science/security area, and more good work is being done every day, but we need a great deal more. I want to point up two key areas in which behavioral science tools are needed in support of the security mission:

1. To cope with human response to equipment-related problems, and

2. To economically and easily predict response under great stress.

Let me give you some scenarios which will pinpoint the problem.

(At this point, four threat-dependent scenarios were presented, involving security at nuclear storage sites. The first involved non-technical electronic security systems alarm-generation until the guards began to ignore the alarms; and the second involved more sophisticated technical alarm generation which produced the same result. Once the guards turned off the alarms or began to ignore them, the adversaries were able to act. In these theoretical scenarios they were able to make off with a nuclear weapon, which was ultimately delivered to Muammar Qaddafi. The next two scenarios involved actions of individual guards when faced with situations such as a peaceful demonstration which is then redirected into a violent attack on a site and a teen-ager who penetrates the site on a prank, resists capture, mouths off, and is beaten. The full scenarios are not included so as to not widely expose potential vulnerabilities.)

The point of the scenarios which I have described is that there are many types of incidents which could produce the type of public attention, social and political pressure which could result in national leaders being forced to take actions which would negatively impact on the deterrent balance so important in the "battle for peace." Those responsible for the security of these nuclear assets so important to this balance need every possible tool which can be provided if they are to succeed in this critical mission.

Guard-force personnel will ignore alarm systems which false alarm or which are induced to alarm, when there are apparent false-alarm conditions. However, if we, through behavioral science research, can find out more about this human response to perceived equipment failure, perhaps we can, if not eliminate, certainly reduce the impact of the problem. Since we are using electronic security systems and there are x number alarms within a short period of time, all of which are identified as false alarms, perhaps the system should ring a bell or light a light. An alarm activates in the supervisor's office, in effect saying, "We've got a pattern here and this is the time that the guard would normally tend to turn off the system or ignore it. You better take some action." The point I am trying to make is that we are going to be living with electronic security systems in the security arena in the future. These security systems false alarm and can be induced to alarm in apparently false-alarm conditions. If we ignore this situation, we know that the human part of the security system--the guard, the console operator--will either ignore the electronic system or turn it off. However, it is possible to explore the man/machine interface, the behavioral aspects of that interface, to provide some better insight for security personnel, supervisors and managers. How many alarms in how short a period produce the unacceptable result? How can this effect best be countered? Hopefully, a tool that can be developed and applied, which may not resolve this problem but certainly reduce the impact of it.

The second area is response of our guards during extreme stress. Certainly we want our guards to respond when they are under attack and certainly that is a stressful situation. There are many areas where guard responses to stress are very positive. However, I am certain that if the Chief of the Miami Police Department had known that the police officers--who allegedly beat the motorcyclist, resulting in his death some months ago, and also resulted in the riots more recently--had known that these officers might respond so inappropriately under stress, they probably would not have been performing the kind of duties that they were. Perhaps they might not have even been policemen.

This is the kind of assistance that could be so valuable in the security field also. We need to be able to identify security guards who will respond or could respond inappropriately, perhaps violently so, in these types of stressful situations. If we could identify them economically and easily before incidents happen, we can avoid potentially disastrous publicity and possibly reduce the number of ways our nuclear deterrent can be neutralized.

In summary, the "battle for peace" is vital to our national interest. Our nuclear deterrent is critical to winning that battle. Security is a major factor in keeping that nuclear deterrent viable. Vulnerabilities do exist including those in the areas I have identified: human response to equipment-related problems and prediction of human response under stress. I believe that behavioral science and security practitioners can develop tools to help cope with these problems. I challenge them to do so.

HUMAN FACTORS, THE ERROR OF OMISSION

Robert J. Hall and William C. Hanna

Mission Research Corporation
P.O. Drawer 719
Santa Barbara, California 93102

The purpose of this paper is first to review the application of psychological research to security personnel problems, second to stress the consequences of ignoring human factors in security, and third to discuss the fundamental issues and recommendations that have been derived from our recent research on military security forces.

Answers to the question, "Why, are the behavioral and human factors problems in high risk technologies ignored?" can provide us with some instructive insights for coping with the behavioral issues of security. Does the oversight occur because we have failed to read the right articles, because the information does not exist in the first place, or because it is expensive and difficult to obtain? Our experience suggests that it is the latter. For example, our efforts in conducting a comprehensive literature search were rewarded by a large volume of articles and abstracts. A careful reading of the abstracts and articles left us with the distinct impression that there is very little in the way of behavioral data that can be directly applied to the problems of operational security.

The lack of relevant data for formulating candidate solutions and supporting decisions about behavioral problems is traceable in part to the objectives and methods of laboratory experimentation and the lack of applied behavioral research in the security area. For example, in their study, "Translations and Applications of Psychological Research," Mackie and Christianson (1967) indicated that academic and applied psychologists recognized that they cannot rely uncritically on the results of laboratory experiments to tell us how to solve real world problems.

The danger in generalizing from laboratory experiments to an applied setting, such as security, is that the laboratory is a highly contrived and artificial situation in which a few highly controlled factors of interest to the experimenter are allowed to vary, while other factors that occur in the real world are neutralized or suppressed. As a result, psychological experiments conducted in the laboratory are oversimplified.

The consequences of oversimplified experimental models which avoid real world complexity have been the cause for much of the criticism and dissolutionment with behavioral research. Chapanis (1959) and Simon (1977) suggest that the traditional experimental method has failed because it looks at too few variables in a single experiment and collects far too much data for the number of effects that must be estimated. Because such studies fail to account for much of the performance variability that would occur outside the laboratory, the effects and statistically significant results of laboratory experimentation are often trivial.

In the applied setting, the behavioral researcher cannot afford to ignore individual differences. Instead, he must seek to describe and predict the behavior of the individual in his environment. He must address what happens in specific situations with practical boundaries. He must study the relationship among multiple independent and multiple dependent variables while seeking to consider all sources of variance that might affect the behavior under consideration in a specific task. The road map for applied behavioral research (solving real world problems) in areas such as security must start with the big picture and then through a series of iterative steps proceed to bound and describe the most important problems and then to identify the information required for candidate solutions. Figure 1 outlines the phases, goals, methods, and anticipated results of an applied behavioral research strategy for security. This figure which illustrates complexities, time requirements, and cost of applied behavioral research provides a partial explanation for the lack of relevant and useful behavioral information. However, the limited relevance of laboratory experimentation and the potential cost of research in the operational setting should not minimize the importance of controlling human error and sustaining operator performance in high-risk technologies (Senders 1980). To system designers, expected human behavior remains a problem in the face of inconclusive behavioral research data.

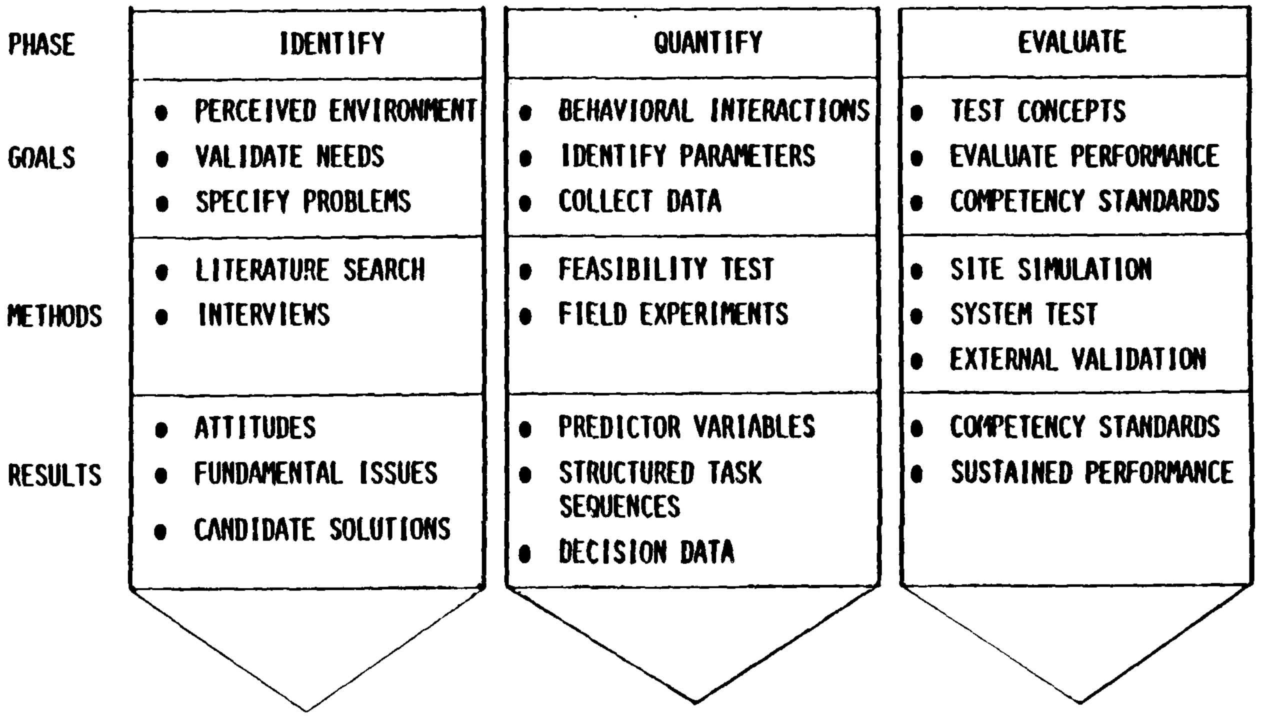
THE CONSEQUENCE OF IGNORING THE PROBLEM

Confronted with the uncertainties of behavioral data, many engineers and designers have concluded that the prudent approach is to design the human out of the system. The title, "Human Factors, the Error of Omission," is intended to suggest that, in the absence of documented and readily available human factors data, the choice has been to sidestep problems that require new behavioral information.

Although it is accepted that military security systems will remain people intensive for many years to come, military project managers and the researchers have chosen to concentrate on the design of security equipment. Research on new sensors and automated response systems are conceptually simpler, the results have high visibility, and the research products are predictable and easier to defend and demonstrate than those of behavioral research. The present credibility gap for behavioral and human factors research is documented by the lack of research that integrates men and equipment and the budgetary avoidance of behavioral issues.

Designs that attempt to remove human error through automation usually retain the operator as a backup system that must take over when hidden malignancies in the design cause the system to crash. As an infrequently used backup system, the human operator has a high probability of failure because:

1. It is unlikely that he will recognize a complex and unique system malfunction until it is too late.



PHASE	IDENTIFY	QUANTIFY	EVALUATE
GOALS	● PERCEIVED ENVIRONMENT ● VALIDATE NEEDS ● SPECIFY PROBLEMS	● BEHAVIORAL INTERACTIONS ● IDENTIFY PARAMETERS ● COLLECT DATA	● TEST CONCEPTS ● EVALUATE PERFORMANCE ● COMPETENCY STANDARDS
METHODS	● LITERATURE SEARCH ● INTERVIEWS	● FEASIBILITY TEST ● FIELD EXPERIMENTS	● SITE SIMULATION ● SYSTEM TEST ● EXTERNAL VALIDATION
RESULTS	● ATTITUDES ● FUNDAMENTAL ISSUES ● CANDIDATE SOLUTIONS	● PREDICTOR VARIABLES ● STRUCTURED TASK SEQUENCES ● DECISION DATA	● COMPETENCY STANDARDS ● SUSTAINED PERFORMANCE

Figure 1. This long-term view of security behavioral research identifies the temporal relationship (what comes first) between research objectives and methods. It provides an overview of a behavioral research strategy that moves in the direction of problem quantification and the evaluation of candidate solutions, all of which exceed the cost and complexities of the traditional laboratory approach.

2. Because he is a backup, he gains little experience or practice in doing what he is supposed to do.

3. The more reliable the machine he supports, the less likely he will respond appropriately.

A recent example of these concerns was expressed in a review of the fully automated cockpit that will fly the new transports from portal to portal.

The cost of ignoring human deficiencies in equipment design, training, and operating procedures has been clearly established by the Three Mile Island disaster, where the Kemeny Commission reported that the equipment worked reasonably well, but the operators did not (Senders 1980). Thus, the consequences of ignoring the lack of understanding of expected human behavior in critical situations will be a continuing high probability of system failure due to human error.

TRADITIONAL ISSUES

Survey and interview techniques are a traditional approach for scoping the big picture and getting at traditional issues. At the last Symposium, I presented a brief report which presented the results of comprehensive interviews with security personnel (30 Air Force and 175 Army personnel). Topics covered during these interviews included job descriptions, attitudes toward job, site characteristics, security equipment, and operational procedures. Traditional issues reported by the security personnel included frustrated job expectations, boredom, shift duty, and negative attitudes of civilians and other military personnel. Other findings which question the effectiveness of current security personnel include questionable proficiencies in weapons and tactics, uncertain leadership, unrealistic training, uncertainty concerning the use of deadly force, and the belief that security is a dead-end career populated by second class citizens. An analysis of the traditional issues suggests that they are symptomatic of more basic causes and forcing functions.

FUNDAMENTAL ISSUES

Poor motivation is inherent in the security job structure, and we cannot expect occasional training activities to cope with the day-after-day boredom and negative attitudes that are a part of present security tasks. Cosmetic changes, e.g., more time off, better barracks, etc., will not change the nature of the job. Basic changes in motivation are predicated on techniques that can modify and restructure the security job.

There is no observable or recorded performance product on which to judge the performance of security personnel. Negative attitudes toward security personnel are supported by the frequent observation that security police do not produce anything. Much of the security job is difficult to quantify because it consists of search and scanning of unpredictable and unique events such as perimeter and structure alarms caused by the winds. The absence of a traditional work product and the difficulty in measuring search behavior or the responses to unique and uncertain events (alarms) has led to the dependence on performance judgments that are based on indirect measures, such as clean weapons, proper uniforms, polished boots, proper equipment at guard mount, general appearance, etc.

Equipment cannot solve the problem, i.e., equipment that simply replaces one boring task with another inactivity is not a solution. Also, an overdependence on equipment to replace the human operator increases the likelihood of error in the event of equipment failure and emergencies.

Response readiness is uncertain because security personnel lack the opportunity to simulate engagements or to prepare a counterreaction response to an armed attack. Their lack of tactical skills includes response action sequences involving coordinated deployment of small tactical units and limited evidence for weapons proficiency. The response readiness of military security personnel are not unlike the personnel at Three Mile Island where the Kemeny Commission found limited and infrequent training for emergency procedures.

The present reward structure is a self-fulfilling prophecy in which the negative attitudes about security duties are extended to security personnel. Results of these expectations about security personnel include a lack of respect by other military and civilian personnel and a belief that those who are the recipients of dull working conditions and uninteresting jobs are second-class citizens. The unfortunate aspects of these expectations is a gradual adaptation and assumption of these roles by the security personnel themselves.

RECOMMENDATIONS

The true test of a critic comes when he is given the opportunity to work on and change that which he has been criticizing. On such occasions, his sudden onset of sympathy and understanding for the problems that must be overcome seems all the more remarkable.

If we are to make cost-effective improvements in the personnel performance, we should recognize that, first, much of the detailed information and data needed is embedded in the operational security systems and much of it may not be generalizable to other sites; secondly, in the final analysis, the skill and techniques designed to sustain and improve security personnel performance must translate into action programs that can be used by the operational units in their day to day functions. Although the behavioral research can aid and facilitate the development and implementation of a program, in the final analysis the program's external validity and success rest with the operational unit itself.

The positive side of security personnel problems is that we do know how to solve and correct most of the fundamental issues that are driving human performance.

We propose three solutions:

1. Vigilance maintenance through simulation

2. Human engineered sensor systems

3. An integrated career program

RECOMMENDATION NO. 1--SIMULATION: A SHORT-RANGE SOLUTION

The use of synthetic or simulated targets to sustain vigilance and observing behavior in sonar and radar systems is an established practice, and the physical simulation of the command control function and emergency procedures provides valuable experience where none other is possible. The proposed use of physical simulation to motivate and sustain the performance of security personnel is very similar to that used in applications. Examples of simulation exercises might include:

1. Random surrogate threats that deal with the individual security guard's performance. Typically, they will be concerned with simulation of stimuli and events to sustain vigilance (e.g., detection, assessment, tracking of potential intruders, and detection of imposters and contraband).

2. Exercises which deal with small unit tactics. These simulations would seek to create and observe their responses and actions (e.g., deployment of the response force and other one sided tactical games).

3. Simulated engagements involving an intelligent adversary or opposing team (two sided face-to-face competitive games).

Figure 2 provides an example of how the development of a Security Operational Performance and Recording and Analysis System might be constituted.

Simulation exercises for sustaining vigilance and observing behavior would generate surrogate detection, assessment, and tracking tasks. For example, synthetic stimuli could be used to generate surrogate tasks for patrols, static guard posts, tower operators, sensor system operators, and the personnel responsible for portal and circulation control. Detection and assessment exercises could use standardized targets that have been calibrated for different types of search tasks. Recognition tests might include visual recognition of site personnel, auditory recognition of communicators, airborne search, and the use of light amplification and night devices. Exercises involving electronic sensors would include perimeter sensors and CCTV assessment, tests of interior sensors, and duress alarms. Portal and circulation control exercises could involve interior escort exercises, ID tests, and contraband search.

The use of synthetic or controlled stimuli to sustain performance and the employment of t^ctical engagement simulation to maintain response readiness requires (1) procedures and equipment that can introduce synthetic stimuli and events into the security environment, (2) apparatus and procedures for observing and recording performance, and (3) feedback methods (e.g., after action reviews in which the personnel responses and events are reviewed chronologically).

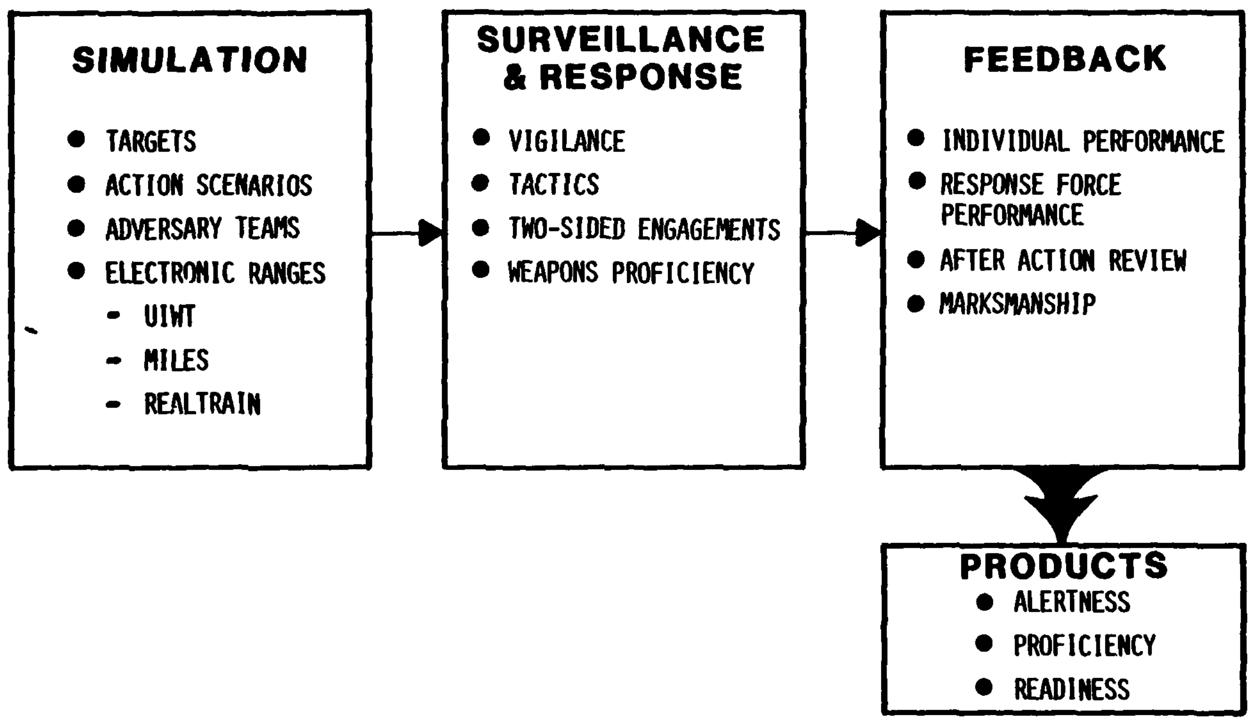


Figure 2. The short-term solution suggests the use of simulation techniques to insure alertness and vigilance, weapons proficiency, and response readiness to emergencies. In addition to motivating and sustaining security personnel performance, the simulation could provide a performance product for identifying security skills and standards.

The development of the Security System Operational Performance and Recording Analysis System (SSOPRA) reported on by Dr. Mackie of Human Factors Research is an example of an operational data sampling model for observing and recording the information which passes through the communication network of an operational nuclear site. The unique aspects of this approach involve the utilization of the operational communication network and the development of a flexible apparatus and methodology for sampling and recording data from the radios, telephones, sensors, and voice communications at the site.

Higher levels of simulation could include competitive two-sided engagements in which teams or platoons would engage in simulated actions that include the responses of an intelligent adversary played by one of the test teams. Surrogate tasks could provide measures of response force performance including detection assessment timelines, deployment interdiction timelines, use of cover and concealment, and casualty exchange ratios. Data derived through such surrogate exercises would include individual speed and accuracy scores and cumulative records (e.g., vigilance, weapons proficiency, etc.), a review of small units' responses to scenarios (e.g., video tapes, observations), and after action reviews in which the exercise is reviewed by each of the operational and adversary teams.

RECOMMENDATION NO. 2--HUMAN ENGINEERING AND SENSOR SYSTEM DEVELOPMENT: THE LONG-RANGE SOLUTION

The result of careful human engineering during the sensor system development should produce a partitioning of tasks between men and equipment in which functions are distributed according to the talents of the men and machines. For example, we would expect the initial sensing and alerting functions to be assigned to machines and the decision functions, such as signature analysis and pattern recognition, to be the responsibility of the security personnel.

The identification of pattern recognition processes and the operational definitions of resolution requirements using human operators should be included as part of sensor system development. A human engineering evaluation and testing the sensors (sonar, acoustic, vision, radar, CCTV, IR, etc.) under development could determine the resolution required to perform a representative set of security tasks at given ranges and under representative weather and terrain conditions. It would be interesting to know what the performance characteristics of imaging sensors are for identifying site personnel with a 95 percent accuracy at ranges of 10-200 meters. The research suggested here is development of a program that would provide human engineering data for sensors and target signatures at representative ranges.

In addition to evaluating the system on representative tasks, human engineering can aid the designer by providing information on the comprehensiveness of signal representation and display needs. For example, does the system provide display output that contains sufficient perceptual dimensions (color, shades of gray) and a range of stimulus attributes that represent the information available in the sensor signature (e.g., can the display handle the distinguishing features of the signature and does the target signature contain sufficient information to enable the human observer to discriminate complex targets at the display?).

Human engineering data can aid the designer in specifying display dynamics and in the manipulation of sensor data for the development of tunable or focusable sensor systems (for example, is the cost of increased resolution, additional scanning and focusing of high resolution sensors significant or justified in terms of improved detection, assessment, and tracking of intrusions?). In short, the specification of sensor tests and their interaction with the human operator is an important part of the contributions that can be made by the behavioral scientist.

RECOMMENDATION NO. 3--THE CAREER SOLUTION

To provide for motivation and effective skills development, a security career must have utility for the individual's development. In some instances, career growth could be facilitated by a restructuring of the security personnel system. Suggested changes include:

Establishing a Professional Security Force in which the security professional is recognized as an individual with a specific set of skills and internalized standards. Recognized security assignments would include critical security duty (e.g., critical resources such as nuclear, biological, and VIP's and security crises such as terrorists, attacks, riots, and hostage situations).

The Development of Competency Based Performance Standards. The use of normative instruments such as intelligence or aptitude tests for measuring performance (real or expected) is questionable, particularly in security situations where physical competence or mastery decisions based on knowledge are required. It is proposed that security training employ a criterion-reference measurement system that will determine when levels of competence are being met. In many instances, this will require the development of an external criterion against which post training performance can be assessed. The objective of criterion-referenced tests is to measure what the trainee can do, or must know, in order to complete a task successfully. Criterion-reference measurement is interpreted against a standard and the performance data provides information on mastery of practical tasks. Such tests may yield a restricted score distribution (i.e., certified/not certified, go/no go).

Make the Operational Unit Responsible for Training. Security training would become the responsibility of the operational unit. Under an apprenticeship concept, security training would be treated as a continuous process in which the attainment of weapons proficiency and tactical skills becomes the primary responsibility of the organization to which the individual is assigned. The major part of all security training will occur within the unit to which the individual is assigned, and new personnel could be integrated into new units when the unit is in a training cycle.

Provide On-Site Adversary and Test Capability. The addition of a continuous training and assessment function requires the addition of an adversary or training unit that is integrated with normal operations, for example, a unit rotational system in which one unit would function as the adversary or test unit for the four units remaining on security duty.

Make Operational Inspections Relevant. The development of security inspections that are realistic and productive in their contributions toward improving the performance of security personnel is essential. Inspections should be composed of security specialists who function as management consultants and advisors to the site personnel. Site evaluation should be based upon operational performance rewards that are related to basic security skills (e.g., weapons proficiency, small unit tactics and communication, engagement simulation, language specialties, circulation control, mob control, hostage negotiations, explosives and biological agents).

The most effective and efficient means for immediate improvement in security is through better utilization of security personnel. Dramatic improvement in security personnel are dependent on behavioral factors such as certification of weapons proficiency, simulation whereby output of security personnel can be verified and rewarded during normal security operations, performance competition between units, and unit pride and cohesiveness. Simply stated, security personnel should continuously train and be evaluated for what they are expected to do, i.e., (1) the detection, assessment, and tracking of potential threats and (2) the response to crises and active security threats.

REFERENCES

Chapanis, A. T., "Relevance of Laboratory Studies to Practical Situations," Ergonomics, 10, 1967, pp. 557-577.

Hall, R. J., et al., Security Personnel Performance Measurement System, Vol. 1, Overview of Phase II, Results and Recommendations, MRC-R-513, August 1979.

Hall, R. J., et al., Security Personnel Performance Measurement System, Vol. 2, An Extended Discussion of Phase II Procedures, Results and Recommendations, MRC-R-513, August 1979.

Hall, R. J., at al., Security Personnel Performance Measurement System, Phase I, Literature Search and Data Collection Design, Final Report, Vols. 1 and 2, MRC-7845-2-179, February 1978.

Hall, R. J., et al., The Impact of Security Equipment and Sensors on Security Guard Peformance, published proceedings of the 1980 International Conference: Security through Science & Engineering, 23-26 September 1980, West Berlin Technical University, West Berlin, West Germany.

Mackie, R. R. and P. R. Christensen, Translations and Application of Psychological Research, Santa Barbara Research Park, Goleta, Calif: Human Factors Research, Inc., Tech. Rep. 716-1, 1967.

Senders, J. W., "Is There a Cure For Human Error?" Psychology Today, April 1980, pp. 52-62.

Simon, Charles W., New Research Paradigm for Applied Experimental Psychology: A System Approach, Canyon Research Group, Westlake Village, California, October 1977.

VIGILANCE PERFORMANCE OF SECURITY FORCE PERSONNEL

Ann Ramey-Smith and Stephen T. Margulis
National Bureau of Standards
Washington, D.C. 20234

The research being performed by the National Bureau of Standards (NBS) for the Defense Nuclear Agency (DNA) involves two tasks. Overall, its goal is to assess those factors that influence the individual state of vigilance in an effort to identify methods to improve this aspect of guard force performance on a daily and long term basis. The first task in achieving this goal is an investigation of the influences of the work environment on performance. That is, an evaluation will be performed of the factors related to the physical characteristics of the task that affect human behavior. This will involve a human engineering study of the vigilance task of security force personnel. The second task of this project is to study the influences of the social environment on guard force performance. This aspect of the project will involve a social psychological and environmental study of the vigilance task.

These two aspects of vigilance performance, that is, human engineering and social/environmental, are related. Both interact to define the ultimate effectiveness of the guard's performance in a watchkeeping task. However, each is very broad in nature. Consequently, we have selected only a small portion of these aspects for investigation by NBS.

Varied experimental situations historically have been used to study vigilance behavior in the laboratory. These range from simple discrete tasks where an observer must detect onset or offset of a signal to a more dynamic task in which the observer must detect a change in regularly occurring stimulus events (Warm, 1977). All the vigilance tasks have several features in common which are characteristic of the watchkeeping situation:

1. the task is prolonged or continuous,
2. the response of the observer typically has no effect on the probability of occurrence of critical events or signals,
3. the signals to be detected are usually clearly perceivable when the observer is alerted to them, and
4. the signals occur infrequently and aperiodically (McGrath, 1963).

The watchkeeping task of the physical security guard at a nuclear storage facility clearly falls within the realm of vigilance tasks.

Vigilance research has broad applicability to fields other than military watchkeeping. Human vigilance is very important to industrial inspection and quality control. The vigilance phenomenon is of concern also in an "...on-going process, such as a power plant, patient in an intensive care unit, or radar air traffic control center, or a battlefield. The systems are usually automatically controlled -- the monitor is not concerned with moment-to-moment manipulations or decisions, but remains as a watchkeeper over the displays, on guard against indications of abnormal conditions" (Weiner, in press).

The problem of human monitoring in industrial and applied settings is indeed much more complicated than in the traditional laboratory vigilance task. It can be argued, however, that many of the same principles which enhance vigilance in the laboratory setting are applicable to contemporary complex monitoring tasks.

So, human vigilance and monitoring activities range from visual inspection of a single attribute of a manufactured product to the complex task of monitoring in a nuclear power plant. It is our hope that the findings of the research proposed here to investigate the vigilance phenomenon in the military, physical security setting will be applicable to these other areas that require a vigilant human operator.

Those interested in a review of the theories that have been proposed to explain vigilance as well as a discussion of the application of vigilance research to nuclear security will be interested in an NBS sponsored report on the subject prepared by Human Factors Research, Inc. entitled, "Vigilance Research and Nuclear Security: Critical Review and Potential Applications to Security Guard Performance," NBS GCR 80-201, June 1980.[1]

A variety of response measures have been used to measure vigilance performance. Among those measures often used in studies of vigilance are:

- response latency,
- observing responses,
- percent correct and incorrect detections,
- measures of signal detectability and cautiousness in reporting, and
- physiological measures.

[1] Available from the National Technical Information Service (NTIS), Springfield, Va. 22161.

Performance on a vigilance task is influenced by three types of factors: task, organismic, and environmental. Environmental factors include, for example, noise, temperature, and ambient lighting. Organismic variables include individual differences and abilities that may be related to vigilance performance.

Task variables include signal rate, background event rate, knowledge of results, time-on-task, and signal complexity, to mention a few. Defining a few terms, signal rate refers to how frequently a signal, in this case an intrusion, occurs. Background events are the repetitious background non-signal stimuli in which the signal occurs. Signal complexity refers to the dimensionality of the stimuli; that is, the signal may vary from the background events along one or more dimensions.

The vigilance task of guard force personnel is characterized by a low signal rate in that the incidence of intrusions is slight. The watchkeeping duty is prolonged in nature. The background event rate varies, dependent upon site differences from being very low, as in a rural storage site, to very high, as in an urban center. The vigilance task also varies considerably depending upon the duty the guard is performing. That is, a tower guard's task is different from that of a guard in a control room monitoring an intrusion detection system.

NBS research on task variables will address these issues. At this time we are developing an experimental plan to be submitted to DNA. The following describes the proposed future research.[2]

We envision a 4x3 factorial design to investigate the effects of signal probability and task differences. Subjects will be presented with four levels of signal probability in a simulation of the guard post. Three types of guard duties will be simulated: first, a tower watch where no control panel is present; second, a control room where the guard is alerted by a visual light display and must perform a visual search of the compound; and third, a control room where the guard is alerted by light signals but assesses whether an intruder is present through a series of television monitors. Subjects in each of these groups will be shown video tapes of a compound perimeter on which the signal rate (i.e., intruders), and background event rate (i.e., pedestrians, animals, and other non-signal stimuli) are varied. In this way the signal probability will be manipulated.

[2] The final research plan, as prepared for future DNA use, differs from that described here.

The subjects' performances will be recorded over an eight-hour period. Dependent measures to be taken will include observing responses, such as those measured using oculometric recording techniques, probability of correct and incorrect detections, and other physiological and performance responses.

The design described here is tentative at this time pending verification of our research hypotheses through site visits at several nuclear storage facilities. The laboratory research proposed will feed into field studies to be performed in following years so that our recommendations and guidelines can be validated and alternate methods for enhancing security guard performance developed. There is a mutual interplay between laboratory research and field studies, where some questions are most appropriately addressed in the laboratory and others in the field. No doubt field studies will suggest questions to be explored in the laboratory and vice versa. So by performing both types of research, we should be able to address the factors affecting the vigilance performance of guards.

Social-psychological, organizational and environmental factors affect vigilance as well. This focus complements the typical emphasis on characteristics of the signal and its presentation. The NBS vigilance project is considering this focus because, as Miller and Mackie (1980) note, although "there have been few, if any, attempts to systematically study the impact of social variables on the vigilance performance of watchstanders (,) ... what evidence there is would suggest that the influence of social variables is not trivial" (p.36).

Moreover, based on interviews with military security guards at nuclear weapons storage sites, Abbott (1979) and Hall (1980) both report a variety of social-psychological and organizational problems that may be adversely affecting guard performance. These include some problems arising specifically from watchstanding.

Thus, interview data suggests the relevance of social-psychological factors and a recent, major literature review suggests the need to study such factors. In our view, organizational factors are a category of social-psychological factors. Environmental factors refer here to the physical context within which social and organizational activities take place.

The hypothesized effects of social-psychological factors on vigilance are best understood by using a distinction made in signal detection theory. These factors are likely to affect the reporting of signals. They are less likely to affect the visual acuity of the guard or the visual discrimination of signals (Miller and Mackie, 1980; Weiner, in press). However, environmental factors may affect the visual discrimination of signals.

From the vast array of possible social and environmental factors, we are focusing only on a very few. For example, we are limiting environmental factors to the physical work setting that surrounds and includes the military guard on duty, the military superior who has come to monitor the guard on watch, and any visitors or intruders at or near the guard's location. Conceptually, the environment is regarded as a visual information field (Archea, 1977). For the guard, this information field is a basis for signal detection and for coordinating his behavior with the actual or possible presence of military superiors or intruders (Archea, 1977; Benedikt, 1979; Fineberg, Perry, Morgan, and Woefel, 1979).

Clearly, the detectability of signals is a precondition for accurate reports of signals. Thus, the visual field is important to vigilance. As for a guard using environmental information to coordinate his behavior with that of others, this relates to a possibly important issue in the study of guard force vigilance. The issue can be stated as the distinction between actually being vigilant and only appearing to be vigilant (cf, Margulis, 1979; Scheibe, 1978).

There are many reasons why a guard would be vigilant. A major one is the threat posed by intruders to the guard and to the weapons he is protecting. See Morgan and Larson, 1979, for a scenario of a terrorist attack.) However, according to interviews with security guards, although they recognize the threat posed by terrorists they simply do not believe there is much likelihood of such an attack (Abbott, 1979; Hall, 1980). Thus, guards are left to face the boredom, tedium, repetitiveness, and stress of watchstanding. Guards are required to be alert but their job conditions work against this. Consequently, the guard may become inattentive and unprepared. The threat of being caught unprepared while on watch, by the Duty Officer for example, is a reason for trying to appear to be vigilant when this is necessary. Appearing vigilant, if done successfully, is protection against disciplinary action.

What follows are very brief statements about topics being considered for investigation. We are planning to have research on social and environmental factors follow and build on the principal effort to study characteristics affecting vigilance performance during long-duration tasks.

Topic One: Under exceedingly monotonous, long duration conditions of watchstanding, the attentiveness of a guard and his degree of arousal will reflect (1) the probability that an authority will be present, (2) the ease of monitoring the approach of such an individual, and (3) how exposed the guard's own behavior is to an approaching authority. That is, guards will act vigilant to avoid disciplinary action when faced with an observer during a long-duration, monotonous vigilance task with a near-zero signal probability. Follow-up studies can establish how the predictability, frequency and durat'on of contact with an observer effects attentiveness and arousal.

Topic Two: This topic concerns whether there are behavioral cues that observers use that reliably differentiate between people who are being vigilant and those who are only acting vigilant (e.g., Kraut, 1978). A related concern is to objectively measure and to compare the performance on a vigilance task of guards who are trying to remain alert and those who are only "faking" being alert.

Topic Three: Anecdotes suggest that military authorities have an unfavorable attitude toward false alarms. What is the effect of this organizational factor on reporting of signals? One way to study this is to examine how guards' sensitivity to deception and their expectations of being deceived by visitors affect their private and public evaluations of visitors in a simulated entry post watchstanding task. The effects of how suspiciously visitors act or appear, of the tolerance of one's superiors for false alarms, and of receiving feedback on the accuracy of one's reports could be considered.

The following topics address other aspects of vigilance. One examines whether strengthening the belief that signals are occurring will result in increased attentiveness on a vigilance task with an objectively low signal probability. This topic is based on research which suggests that subjective probabilities of events can be increased by making the event more familiar, memorable, or imaginable (Lichtenstein, Slovic, Fischhoff, Layman, Combs, in press).

Another topic examines the effects on vigilance performance of individual versus shared responsibility for watching for events. Under certain organizational conditions, teams have been found to outperform individuals on vigilance tasks (Morrissette, Hornseth and Shellar, 1975). The question is whether there are organizational conditions that will not only improve vigilance, compared with the individual observer case, but which also respect manpower limitations affecting guard forces in the military.

The last topic addresses the effects on vigilance of the perceived importance of watchkeeping and of the organizational response to the watchkeeper's performance. The study is predicated, in part, on the observation that there is a generally unfavorable attitude in the military toward physical security and toward its personnel, an attitude that suggests that this work and these people are not as important or as valuable as other work or personnel. Hall (1980) reports that security personnel have come to believe this evaluation about themselves. Because of the complex nature of job performance, the analysis of job importance and organizational response to performance should take into account additional social/organizational factors, such as the nature of the control system in the organization (Lawler, 1976), the effect of one's immediate work group on the individual worker (Hackman, 1976), and job satisfaction (Locke, 1976).

In summary, in addition to investigating the influence of the physical characteristics of the vigilance task, studies of vigilance under conditions of objectively low signal probability and of long duration may be conducted to determine the impact of social, organizational and environmental factors on vigilant behavior. The choice of parameters for investigation will be based on results of interviews with security guards, on observations by DNA staff, and on our own analysis of conditions that might be affecting guards on watch. The aim is to better understand guard force performance on a vigilance task so that guard performance can be strengthened and enhanced in the field.

BIBLIOGRAPHY

Abbott, P. S., Candidate assessment. Phase I: Perceptions and job environments of physical security personnel. (Final draft report: Abbott 22500FR). Alexandria, VA: Abbott Associates, Feb. 1979.

Archea, J., The place of architectural factors in behavioral theories of privacy. Journal of Social Issues, 1977, 33(3), 116-137.

Benedikt, M. L., To take hold of space: Isotists and isovist fields. Environment and Planning B, 1979, 6, 47-65.

Fineberg, M. L., Perry, M. E., Morgan, J. H., II, and Woefel, J. C., Analysis and Testing Requirements for Perimeter Barriers and Light Development. McLean, VA: The BDM Corp., Oct. 1979.

Hackman, J. R., Group influences on individuals. In M. D. Dunnette (Ed.), Handbook of Industrial and Organizational Psychology. NY: Rand-McNally, 1976.

Hall, R., Security performance measurement methodology. In G. Lapinsky, Jr., S. T. Margulis, and A. Ramey-Smith (Eds.), The role of behavioral science in physical security. Proceedings of the Fourth Annual Symposium, July 25-26, 1979. (NBSIR 81-2207(R). Washington, DC: Nat. Bur. of Stand., 1981 February.

Kraut, R. E., Verbal and nonverbal cues to the perception of lying. Journal of Personality and Social Psychology, 1978, 36(4), 380-391.

Lawler, E. E., III., Control systems in organizations. In M. D. Dunnette (Ed.), Handbook of Industrial and Organizational Psychology. NY: Rand-McNally, 1976.

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., and Combs, B., Judged frequency of lethal events. Journal of Experimental Psychology: Human Learning and Memory, in press.

Locke, E. A., The nature and causes of job satisfaction. In M. D. Dunnette (Ed.), Handbook of Industrial and Organizational Psychology. NY: Rand-McNally, 1976.

Margulis, S. T., Privacy as information management: A social-psychological and environmental framework. (NBSIR 79-1793). Washington, DC: Nat. Bur. of Stds., Sept. 1979.

McGrath, J. J., Some problems of definition and criteria in the study of vigilance performance. In D. N. Buckner and J. J. McGrath (Eds.), Vigilance, a symposium, 1963, NY: McGraw-Hill, 227-237.

Miller, J. C., and Mackie, R. R., Vigilance research and nuclear security: Critical review and potential applications to security guard performance. Goleta, CA: Human Factors Research, Inc., NBS-GCR 80-201, June 1980.

Morgan, J. H., III, and Larsen, E. B., An evaluation of perimeter barriers and lighting effectiveness. (BDM/W-79-301-TR) McLean, VA: The BDM Corp., June 1979.

Morrissette, J. O., Nornseth, J. P., and Shellar, K., Team organization and monitoring performance. Human Factors, 1975, 17(3), 296-300.

Scheibe, K. E., The psychologist's advantage and its nullification. American Psychologist, 1978, 33, 869-887.

Warm, J., Psychological processes in sustained attention. In R. R. Mackie (Ed.) Vigilance: Theory, operational performance, and physiological correlates. NY: Plenum, 1977, 623-644.

Wiener, E. L., Vigilance and inspection. In J. S. Warm (Ed.), Sustained attention in human performance. NY: Wiley, in press.

THREAT ASSESSMENTS....

"Horse Before the Cart"

Patrick R. Lowrey
Cypress International, Inc.

INTRODUCTION

A threat assessment is a detailed risk analysis of an organization or system to determine weakness in security or survivability. Assessments include checklists and analytical methods for gaining the raw data necessary for the comprehensive analysis.

In too many instances, organizational managers and governmental officials place the "cart before the horse" by purchasing security products and security services without the needed analysis of risks and vulnerabilities, i.e., the threat.

Most organizations have funds allocated for security but often unintentionally fail to allocate time and effort to assure the development and implementation of a cost-effictive program. A poor security program is worse than none at all because the organization is lulled into a false sense of security. A well-conducted threat assessment based on an efficient methodology is without doubt the most cost-effective way of achieving a long-term successful security and survivability program. The analysis of raw data is essential to both the development and implementation of protection programs, and correcting programs that are unsophisticated, unproductive or disorganized.

MATERIEL ACQUISITION AND THE EVOLVING THREAT

In the materiel acquisition process, again we find the "cart before the horse" in terms of threat assessments.

THE NEED FOR NEW MATERIEL

New materiel requirements in the military services are generated by recognized mission area shortcomings resulting from changes in doctrine, operational deficiencies, or new technological opportunities. The development of these requirements is influenced by international events and by the many players in the materiel acquisition cycle.

The requirement to meet a materiel shortcoming is expressed in the form of a requirement document. The type of document differs depending on fiscal thresholds, level of interest, and stage of development. The proper document is prepared and staffed with appropriate Defense Department agencies. The combat developer, materiel developer, and military service headquarters are each charged with certain definite responsibilities at each stage of the materiel acquisition process.

BASIC POLICY AND PROCEDURAL GUIDANCE

Policy and procedural guidance are enunciated across a broad base of higher authority and internal DOD issuances. Key milestone and decision points that are basic to the acquisition process are provided by the following:

- OMB Circulars A-11, "Preparation and Submittal of Budget Estimates"; A-76, "Policies for Acquiring Commercial or Industrial Products and Services for Government Use"; and, A-109, "Major Systems Acquisition".
- DOD 5000.1, "Major Systems Acquisition"; and 5000.2, "Major Systems Acquisition Process".

KEY PLAYERS

Key decisions on major weapon systems are made by the Secretary of Defense. In fulfilling that responsibility, the Secretary is provided advice and assistance by the Defense Systems Acquisition Review Council (DSARC).

The program manager is the person assigned responsibility by the DOD Component Head for a new program. He briefs the DSARC at key decision points in the acquisition process.

THE APPROPRIATION PROCESS

The annual appropriation process overlays the acquisition process and is an integral part of it. The underlying objective of the appropriation process is to examine the annual statement of the acquisition plan (strategy) in resource (people, time, and dollar) terms. As a part of this process, established requirements (military needs) are expressed in terms of annual and succeeding year cost objectives (budgets).

THE ACQUISITION PROCESS

The materiel acquisition process is a deliberate sequence of activity and decisions. It is achieved through the application of resources made available through the U.S. Government annual appropriation process. In the DOD, the acquisition process is reconciling mission needs with capabilities, established priorities and acquired resources. The process is different for each acquisition. There is no universal standard for application. Each system acquisition requires a tailored process.

The underlying objective in each phase of the acquisition process is the refinement and quantification of economic, technical, logistic, production, procurement, and evaluation considerations. The phases and basic premise for each phase depicted in Figure 1 of the acquisition process are:

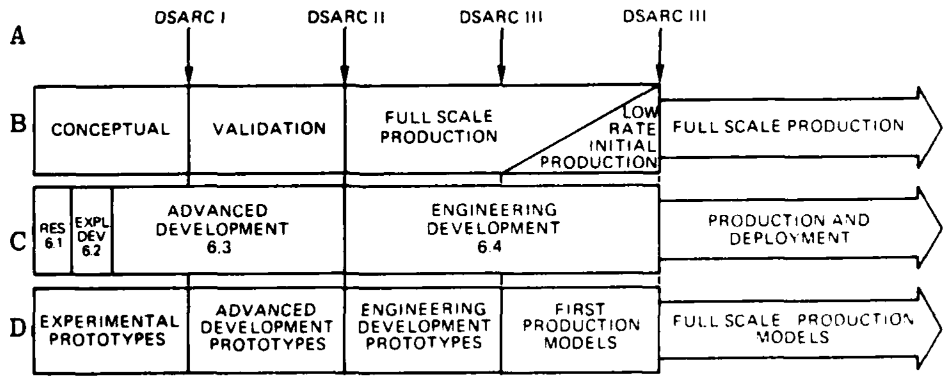
> Conceptual Phase. The technical, economic, military usefulness, broad management, and acquisition approaches are established, and the program is formally initiated.
>
> Validation Phase. The initiation decision baselines are refined through the analysis and quantification of alternative design concepts, and preferred (least risk) solutions are established to reaffirm the need.

Engineering Development Phase. The total system (including support) is designed, fabricated, and tested for operational worth to establish the basis for the production decision and the use of production resources.

Production Phase. The total system (including its support) is production engineered, fabricated with production tooling, and fully tested for operational worth. The operational system and its support are produced and delivered to inventory. When inventory objectives are complete, the program is trasitioned to commodity management.

System Deployment Phase. Concurrent with full production, inventory items are delivered to operating forces. User reports establish modification (retrofit) and overhaul requirements, and the system is operated and maintained until classified as obsolete.

THE MATERIEL ACQUISITION PROCESS



A = Major Program Review
B = Phases
C = Program Funding Source
D = Hardware Configuration

Figure 1

ACQUISITION STRATEGY/PLANS (AS/Ps)

The program manager develops AN/Ps as soon as feasible after program initiation. Strategy is developed using the best available advice from business and technical advisors and from persons experienced in the management of other programs fulfilling similar mission deficiencies. Strategy is composed of general concepts for handling technical, business, and programmatic matters pertaining to the management of a major system. Plans provide the detailed methods for fulfillment of strategy. Together, they consitute a systematic and disciplined way to achieve an effective management process.

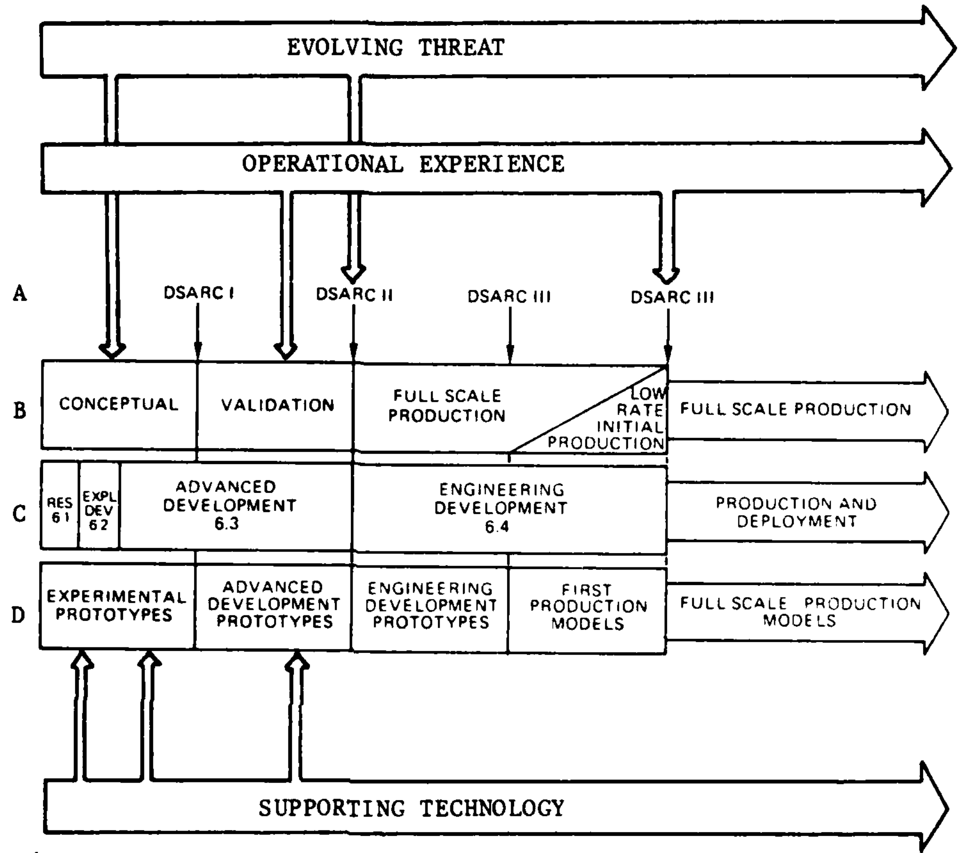
Plans generally involve requirements relating to a broad horizontal range of functional specialties (e.g., contracts, financing, engineering, testing, production, and logistics) and a vertical range of management echelons. These are developed in coordination with appropriate specialist and management staffs.

The program manager considers the requirements of functional and management groups; however, since the program manager is personally responsible for meeting program goals relating to Initial Operational Capability (IOC), performance, and affordability, he has final authority to tailor program requirements to meet assigned goals. Therefore, the program manager has both the authority and the responsibility to overrule staff advisors if necessary. His actions are reviewed during DSARC reviews.

In recognition of the complexity of special functional requirements including threat analysis, the DOD Components' staff capability assists program managers in the blending of requirements into cohesive plans. Special emphasis is placed on the appropriate time within the acquisition life cycle for the introduction of special requirements.

The front end of the acquisition cycle is essentially an information seeking period. It is a period of high technical uncertainty as compared to the period of technical activity which follows during development and production. Figure 2 depicts the three main streams of continuing activity and knowledge gathering: "Operational Experience"; "Supporting Technology"; and, "Evolving Threat". Close interaction is essential to identification of mission need of a program and orderly progress through the development cycle.

THE MATERIEL ACQUISITION PROCESS



(Explanation of A thru D: See Page 4, Figure 1)

Figure 2

"Operational Experience". Operational experience resides in the user organizations, such as the armored or artillery forces of the Army, the submarine force of the Navy, or the tactical aircraft elements of the Air Force. This operational experience is accumulated through actual combat, training exercises, identification of deficiencies in current capabilities, field experiments with new hardware and new techniques, simulation methodology, and doctrinal analysis and development. During periods of peacetime, the user's competence and the sophistication of his attitude toward advanced technology and doctrine will be directly related to the amount of time and resources he spends (or is allowed to spend) on operational exercises and experiments with new technology and techniques. His competence and attitude in this regard are crucial determinants of the length of the acquisition cycle. The user must interact with the developer and support the program throughout the entire cycle. First, he must be a contributor to the mission area analyses that identify a mission need. Second, he must assist in the evaluation of alternative system design concepts for satisfying a particular mission need.

"Supporting Technology". Another activity that is vital at the front end of the acquisition process is that which maintains and improves our technology base. It includes the 6.1, 6.2, and 6.3A programs under the direct control of the DOD, the contractor IR&D programs, and academic and commercial R&D efforts. This activity is highly decentralized and its usefulness to the development of any system depends on how well it has been funded and how wisely laboratory managers around the country have expended their resources. The further along components and techniques are brought in the 6.2 programs, the shorter will be the time required to develop and demonstrate their feasibility for a particular system application.

"Evolving Threat". The effectiveness and survivability of a proposed weapon system in its intended operational environment is fundamental to the acquisition effort and is considered by the program manager from the outset. To assess this effectiveness throughout the acquisition cycle, the program manager uses validated intelligence data to perform an engineering study of the system and threat interaction. The study is updated for all DSARC milestone reviews. The proposed system is modeled against the entire performance envelope of the threat. This process allows program managers to identify threat characteristics upon which the effectiveness and survivability of the weapon system is dependent. Additional intelligence collection is tabulated in an Intelligence Production Status Report (IPSR) by the Defense Intelligence Agency (DIA) for each system concept. The purpose of the IPSR is to inform the intelligence community of the specific intelligence the program manager needs and when it is needed during the acquisition process.

Thus, the program manager has the opportunity to consider the evolving threat to the security and survivability of his program after the IOC is met.

No single aspect of the threat can be treated in isolation. A thorough security systems engineering process is required in the development of a new weapon and support systems. As the threat assessment evolves, every phase of the materiel acquisition process must be rigorously monitored to eliminate characteristics that would constitute inherent vulnerabilities when the system reaches operational readiness.

The program manager's technical responsibility for security and survivability includes certain aspects of the total security system. Total security, from the user's viewpoint, consists of three principal parts: personnel; hardware; and procedures (software). In practice, these three parts are integrated into a total system of security and survivability.

The cost of physical security systems and survivability measures in terms of money and manpower, preclude maximum protection for every tactical weapon system.

It is not economically feasible or theoretically necessary that systems of every kind and character achieve the same degree of added physical protection. The degree of protection warranted is predicated upon an analysis of three factors: criticality; vulnerability; and user's capability. If the system is both highly critical and highly vulnerable and beyond capability of user to protect, then an extensive physical security system becomes a necessity.

Physical security systems are only part of the overall defense of nuclear weapon systems and special nuclear materiels. Exclusion areas, limited areas, access controls, dispersion of facilities, continuity of operations, shelters, protective construction, defense against direct attack and natural disasters must be blended into a total integrated system of physical security. This blended effort begins with threat assessment during the acquisition process.

THREAT ASSESSMENT

ASSESSMENT NEED

During peacetime, the most serious and continuing threat to DOD priority resources, especially strategic weapons systems, stems from intelligence collection efforts by countries hostile to the U. S. All eastern European countries, the People's Republic of China, Cuba, North Korea, and other Communist countries have intelligence gathering organizations interested in any information concerning the U. S. strategic capabilities.

"Security threats" are potential acts or conditions which may result in the compromise of critical information; loss of life, damage, loss or destruction of system, system components or property; or disruption of the mission of the system.

The DOD Physical Security Program is designed to counteract threats to priority resources posed by groups or individuals acting in an unconventional manner. The program is not designed to defend against the attack of conventional military ground forces.

BASIS OF ASSESSMENT

Threat assessments are made by collecting and evaluating intelligence information of the intentions and capabilities of hostile elements whose activities may impact adversely on the security and survivability of the system. It stresses the known capabilities of hostile elements to damage, destroy or impede the planned use or operational effectiveness of the particular system.

When precise information about a hostile element's capabilities is not available, the assessment is based on experience, reason and logic and is relatively free of opinion. Speculation on the intentions of hostile elements is avoided. The most difficult aspect of threat assessment is the cataloguing of literally thousands of realistic scenarios coupled to a multiplicity of hostile element sources. A question of principal importance is the probability of occurrence once a specific threat source and scenario are identified.

THREAT CATEGORIES

Threats are categorized into two types: natural, and manmade.

Natural. Natural threats are mainly hazards to survivability of the system. These threats are the consequence of natural phenomena. Natural hazards or threats cannot be prevented by physical security measures, but may greatly affect physical security systems and operations. Protective measures must be increased when natural hazards occur. Perimeter fences may be down, protective lights and alarm systems may not operate, patrol vehicles and helicopters may be damaged beyond utilization, and property may be scattered over a large area for easy access by unauthorized persons. Typically, the impacts to be expected from each phenomenon are:

(1) Floods - flooding may result in property damage, destruction of perimeter barriers, and short circuiting of alarm and devices.

(2) Storms (tornadoes, hurricane and lightning) - causing alarm devices to short circuit, causing nuisance alarms, and limiting visibility.

(3) Earthquakes - causing nuisance alarms, possible fires, fallen command, control and storage buildings, and weakening storage facilities.

(4) Winds - disrupting power lines, setting off nuisance alarms, causing hazards with flying debris.

(5) Snow and Ice - blocking mobility of operational sites, runways and patrol roads, increasing response time to alarms, and freezing locks and alarm mechanisms.

(6) Fires and Explosions - causing damage/destruction of natural and physical perimeter barriers, maintenance and assembly buildings and operational systems and facilities.

These effects require immediate reinforcement of the security force and implementation of additional physical protection measures to meet system survivability requirements. Physical security plans must be closely coordinated with emergency and disaster plans in order to assure survivability of the system.

<u>Manmade</u>. Manmade threats include acts of commission of omission, both covert and overt, which could disrupt or destroy the system's effectiveness. Every manmade threat will evolve from one of the following sources:

THREAT SOURCES

Designation	Source
A	Terrorists
B	Sabateurs
C	Espionage Agents
D	Thieves
E	Anti-Nuclear Extremists
F	Environmental Activists
G	Skilled/Well-equipped Intruders
H	Disloyal/Subversive Dissidents
I	Socio-psychopaths
J	Vandals
K	Casual Intruders
L	Unintentional Intruders

Figure 3

Each of these sources are carefully defined as any individual or group of individuals that have potential of being a "security threat".

NATURE OF MANMADE THREAT

In general terms, the nature and degree of the manmade threat will vary widely with the geographical location and the operational environment of the weapons system coupled with characteristics of individuals and groups viewing the system as a specific target. Because of political or social opposition, socio-economic factors, mobility of hostile elements, and group motivation, consideration must be given to the capabilities and tactics of each hostile threat source. The threat to overall operations and individual components of a system varies because of these factors as well as the nature of the weapon and degree of access control. The manmade threats are sub-divided into internal and external.

Manmade threats require the identification, tabulation and evaluation of all conceivable sources defined as having the impact potential on security and survivability of the system.

Internal Threat. User personnel who have intimate knowledge of the weapon and the security system form an internal threat. With nuclear weapons, this threat is generally considered by the DOD and uniformed military services to be a human reliability problem and is addressed by the Personnel Reliability Program (PRP). Susceptibility to this threat is reduced by incorporating personnel security clearance measures and improved hardware engineering and design, system installation, and system operation. Component boxes, covers, and cables should be designed to be less vulnerable to tampering. Communication lines and data links should be provided with tamper detection capability to prevent knowledgeable internal personnel from defeating the system.

The PRP is not providing the human reliability for which it was originally designed. However, this issue is the subject of another paper and not addressed here.

External Threat. Outside intruders may attempt sabotage, espionage, theft, or vandalism. Dissidents may be highly motivated towards reducing confidence in the military establishment, embarrass the U. S. Government, or create a dramatic incident to attract public attention. Some may attempt entry without detailed planning or highly sophisticated equipment. Penetration may be accomplished by considering appropriate time factors, location vulnerability, and personnel/guard presence.

On the high end of the threat spectrum, well-organized terrorist units may use overt force and diversionary actions for purpose of terrorism, paramilitary activity and sabotage. Efficiency, depth of planning, execution, sophistication of equipment, and size of force may vary. Terrorism is a significant threat.

Conversely, on the low end of the threat spectrum, casual intruders will attempt penetration with little or no advance planning and without apparent rationale. These intruders include thrill seekers and individuals who are mentally deranged or intoxicated. While casual intruders represent no military threat in the classic sense, they may inadvertently or maliciously cause considerable damage or create nuisance alarms.

Levels of Threat. The general levels of threat are designated low, medium and high. The weapon system configuration and deployment must account for general threat levels and possible escalations. The security and survivability of the system contains a variety of modules tailored to meet the existing threat and provide the required capability to upgrade security in the event the level of threat escalates. Threat level guidelines are presented in Figure 4. This figure also indicates appropriate levels of response by this security force. As the threat level escalates, requirements for probability of detection, reliability and degree of security required, as well as the speed and intensity of the local security response forces, also intensify.

The desired result in terms of "REQUIRED CAPABILITIES" is a totally integrated and self-sufficient system of security and survivability. In a state of Low Threat Level, the system should be less manpower intensive and more dependent on hardware and software.

A totally integrated security and survivability system is depicted later in this discussion.

THREAT LEVEL

THREAT LEVEL	NATURE OF THREAT	[1] REQUIRED CAPABILITIES
Low	Stand-off or internal surveillance/espionage Minimum/occasional penetration Limited pilferage Nuisance alarms	Deny surveillance and penetration Surveillance of perimeter and critical areas Deter, detect, and apprehend intruders Response by Security Alert Team (SAT)
Medium	Low threat intensified Minor sabotage Continued harrassment Minor destruction Minor dissident demonstrations	Intensify response to low threat Early detection Immediate response by Security Alert Force (SAF) Increase mobility of back-up response forces Identification and apprehension of saboteurs Interface with federal law enforcement agencies
High	Medium threat intensified Organized terrorist attack/armed conflict Major destruction and sabotage Special Nuclear Material (SNM) theft Major demonstration followed by penetration of area or system	Intensify response to medium threat Complete penetration denial Immediate response by back-up response forces Heavy weapons capability initiated Assistance by federal law enforcement agencies or military forces

[1] Collective Integrated Security Requirements

Figure 4

THREAT ASSESSMENT METHODOLOGY

The purpose of a security threat assessment is to identify elements considered to be present and potential sources of threat to security and survivability of the system. An analysis is formulated by evaluating raw intelligence information concerning the intentions and capabilities of hostile elements. Hostile intentions are difficult to assess. It is necessary to identify all hostile elements whose activities and demonstrated capabilities are inimicable to the system.

The assessment of capabilities must be prudent, reasonable and logical. Sepcilation concerning the intentions musc be avoided. For example, damage or destruction of a weapon system could be achieved by a clandestine attack. If the hostile element is assessed as having the personnel, weaponry and the technological capability to initiate an attack, then this capability must be identified in the threat assessment. An analysis which follows this pattern has value because it is relatively free of opinion and conjecture.

Essential Elements of Analysis (EEA). In terms of the security of the system, essential elements of analysis (EEA) must be addressed for each of twelve manmade threat sources. These EEA are shown in Figure 5.

ESSENTIAL ELEMENTS OF ANALYSIS (EEA)

- Distinctive traits of threat source?
- Aims and goals of threat source?
- Alternative scenarios?
- Expertise and capabilities?

Figure 5

The EEA considerations are dynamic, evolving processes depicted in Figure 6.

CYPRESS METHODOLOGY

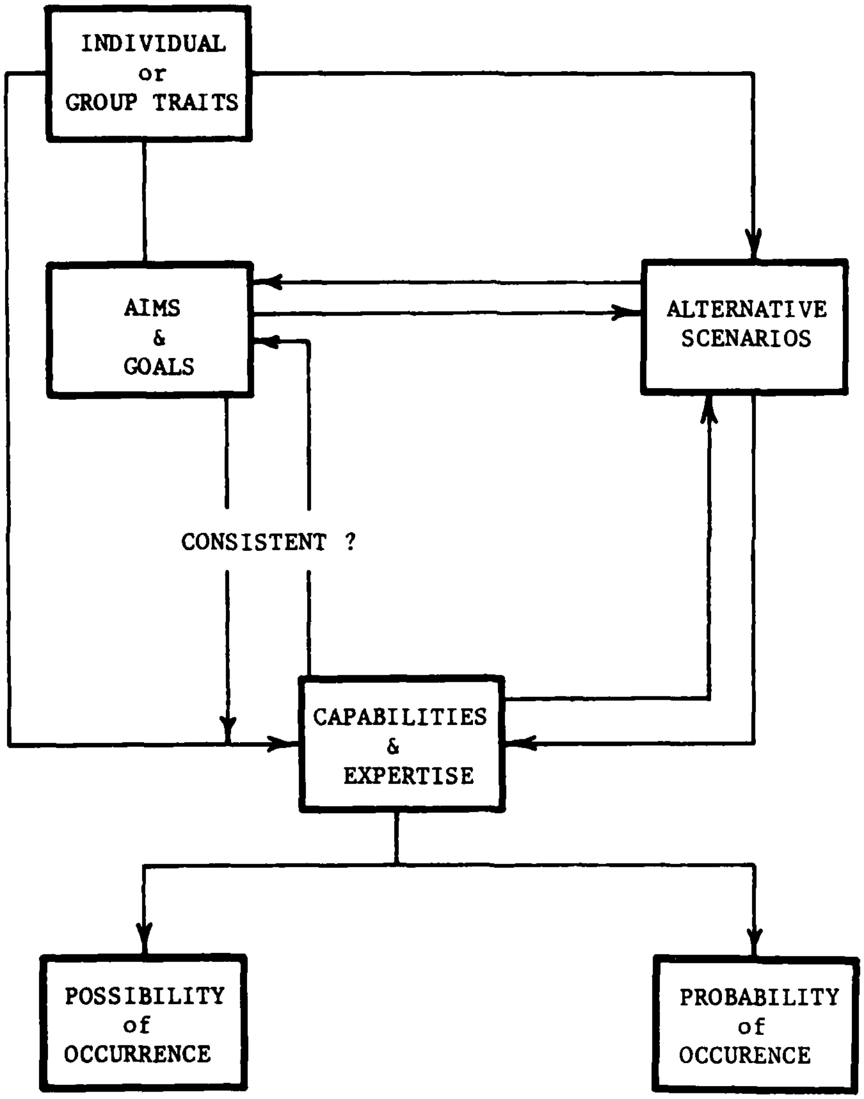


Figure 6

A threat level format shown at Figure 7 provides a summary display of the EEA and permits the analysts to assign relative value judgements in finalizing both possibility and probability of occurrence in all stages of system life cycle management.

THREAT LEVEL ASSESSMENT

MANMADE THREAT SOURCE: (Category of Manmade Threat)

INTERNAL ______ EXTERNAL ______ BOTH ______

ALTERNATIVE SCENARIOS: (Correlation of Traits and Capabilities)

GOALS: (Aim of Individual or Group Threat)

POSSIBILITY vs PROBABILITY	LOW	MED	HIGH
Assessment of capabilities and expertise POSSIBILITY OF OCCURRENCE			
Assessment of consistency among total capability and likely scenarios and goals PROBABILITY OF OCCURRENCE			

Figure 7

For each stage of activity in the life cycle management process, the risks (possibility and probability of occurrence) must be addressed as shown in Figure 8.

THREAT LEVEL ASSESSMENT

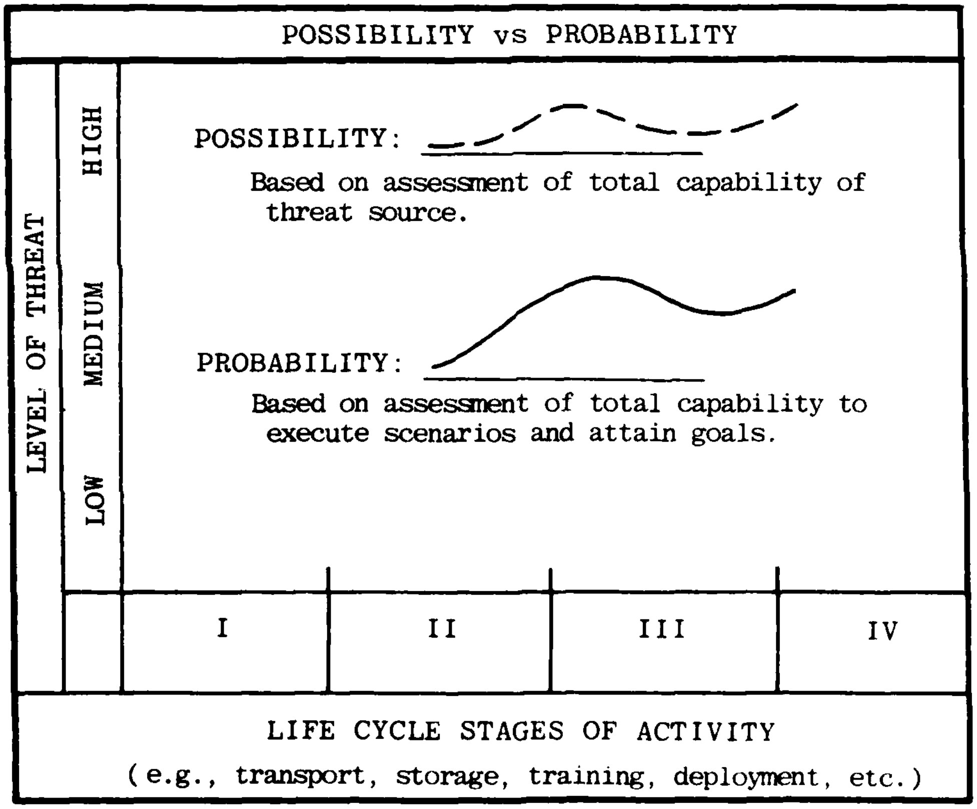

POSSIBILITY vs PROBABILITY
LEVEL OF THREAT
HIGH
MEDIUM
LOW
POSSIBILITY:
Based on assessment of total capability of threat source.
PROBABILITY:
Based on assessment of total capability to execute scenarios and attain goals.
I
II
III
IV
LIFE CYCLE STAGES OF ACTIVITY
(e.g., transport, storage, training, deployment, etc.)

Figure 8

INTEGRATED SECURITY AND SURVIVABILITY

A totally integrated security and survivability system is the ultimate requirement. A portrayal of this concept is shown in Figure 9.

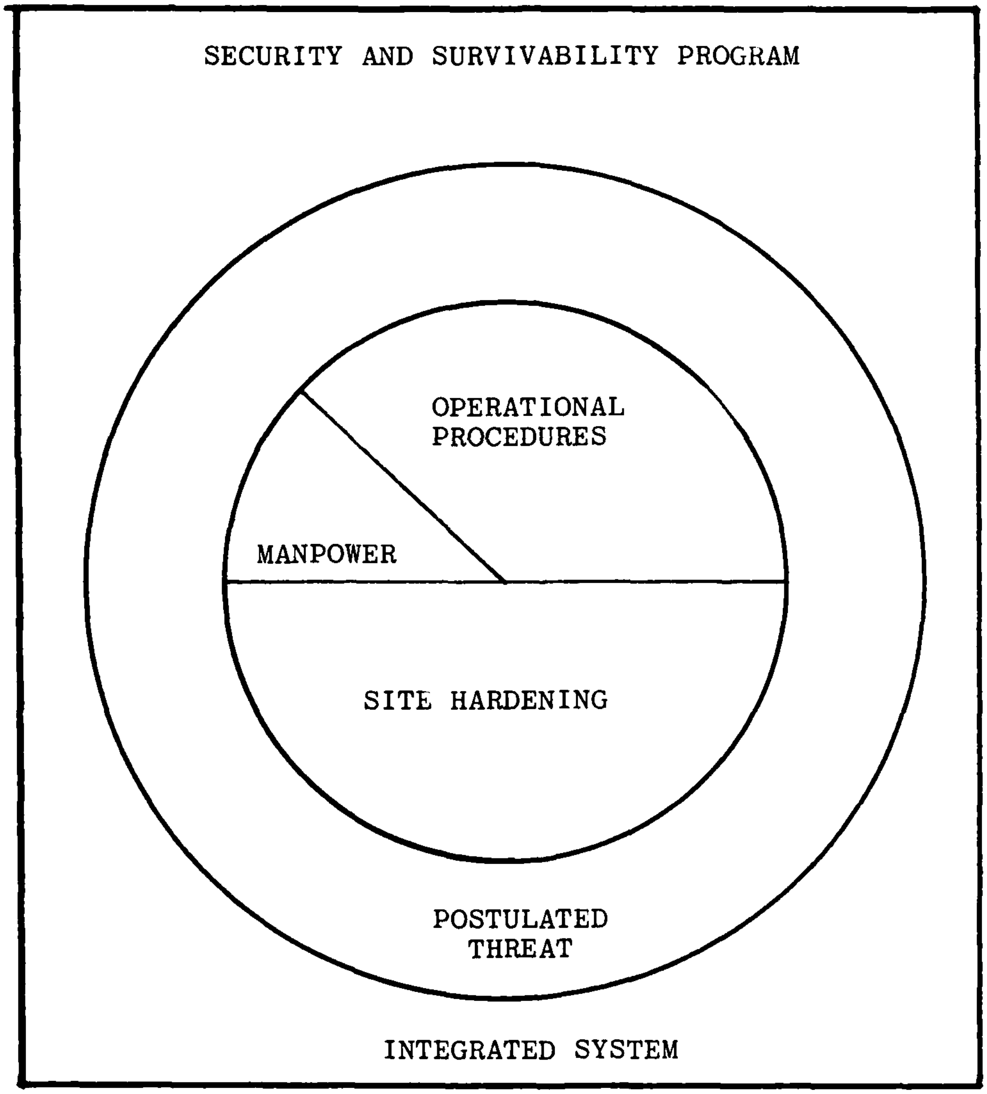


Figure 9

Within the parameters of the threat, the threat analyst must convey a total understanding of system security issues and needs. Only then can the security contractor's design effort contribute to solution of the survivability problem.

A major continuing consideration within the DOD is the need to drive down the requirements for manpower. The design of the security and survivability system must take cognizance of basic manpower, procedural and hardware specifications.

SUMMARY

Threat assessments are exhaustive efforts which must be accomplished prior to fielding a major system. The main purpose of a security and survivability program is to offer the best protection to the system it is designed to protect. A wholehearted assessment effort must be accomplished during the materiel acquisition process.

Although the cost of a security and survivability program is an important factor, it varies with demands for operational efficiency and the stages and components in the system.

DISCUSSION

QUESTION FROM THE FLOOR: You made a plea for the development community to get the users to become more involved in the early stages of development. As an ex-developer, I would like to present the viewpoint of a development community.

The development community does contact, visit, and speak to the user community frequently. But the result we get is always that we go in with an idea, a capability, a technology, and we come back with a group of impossible goals based on no understanding of technology and no perception of how difficult or how physically impossible some of these requirements might be.

So, I would like to say that it goes both ways. The fact that the developer would come in with an often irrelevant system is often the reflection of the fact that the user is not willing to listen to developers' problems.

MR. LOWREY: It is a two-way street.

PSYCHOLOGICAL DETERRENTS TO NUCLEAR THEFT

George Lapinsky
Center for Consumer Product Technology
National Bureau of Standards
Washington, D.C. 20234

In 1975 the Defense Nuclear Agency (DNA) and the National Bureau of Standards jointly conceived the psychological deterrents project as an on-going review of the unclassified and the classified literature relating to psychological factors that may have impact on the design and development of DNA's Forced Entry Deterrent System (better known as FEDS).

Meguire and Kramer initiated work in 1976 with a report of a preliminary review.[1] The present effort, which is nearly complete, is an update of that report.[2] In addition, this latest report will expand into several new areas not directly related to the FEDS system but which nevertheless could be applicable to deterrence of nuclear theft in a more general sense.

Since the field of physical security is an interdisciplinary one, its literature is widely dispersed, and it was necessary to review several data bases and other sources of information for relevant material. These included: National Criminal Justice Reference Service (NCJRS), Psychological Abstracts Search and Retrieval Services (PASAR), National Technical Information Service (NTIS), Defense Documentation Center (DDC) (now known as the Defense Technical Information Center), Sociological Abstracts, Ergonomics Abstracts, Social Science Citation Index, and many isolated documents gathered from the DNA library and other libraries across the country. Some additional information was gathered through personal contacts with authorities in various fields. This search, although thorough, could not be called exhaustive. More work is needed -- especially direct input from experts in the field of physical security.

To date the current review has encompassed over 2000 books, articles, reports and abstracts, both unclassified and classified. The search of the classified literature is presently limited to documents classified SECRET or Confidential. The most recent update of the classified literature was completed in May 1980. Neither the classified nor the unclassified searches have, as yet,

[1] Meguire, Patrick G.; Kramer, Joel J. Psychological deterrents to nuclear theft: a preliminary literature review and bibliography. Nat. Bur. Stand. (U.S.) NBSIR 76-1007; 1976 March. 50 p.

[2] Lapinsky, Jr., George W.; Goodman, Clare. Psychological deterrents to nuclear theft: an updated literature review and bibliography. Nat. Bur. Stand. (U.S.) NBSIR 80-2038; 1980 May. 45 p.

revealed any literature directly documenting any experimentation or empirical data concerning the psychological deterrence of nuclear theft. In fact, very few definitive studies seem to exist relating to the psychological deterrence of any serious crimes, especially those analogous to nuclear theft.

For the purposes of this review, a psychological deterrent was defined simply as anything which is perceived by a potential perpetrator as lowering the probability of successfully attaining his or her goal. (Goal here may also refer to something other than an actual theft, such as embarrassment of government officials or publicity for a political cause.) This definition is based on the general crime deterrence model which hypothesizes that, at least in premeditated crime, the potential criminal intuitively assesses the probability of successfully executing a crime and weighs the possible positive gain against the possibility of failure and the negative consequences.

Two factors, certainty of detection and arrest, and severity of punishment, are central to the deterrence concept. In addition, certain assumptions underly this notion of deterrence -- 1) the adversary must be rational, in some sense of the word; 2) the threat of punishment must be credibly communicated to the potential adversary and must be relevant and important to his or her value system; and 3) the threat of detection and punishment must be above the adversary's risk-taking threshold. Unless a potential criminal feels that there is a good chance of being detected and suffering severe punishment, there will likely be no deterence.

In a sense, psychological deterrence is a form of communication in which the adversary is presented with several alternative courses of action. The problem is to weight these alternatives in such a way as to increase the probability of the adversary chosing alternatives which are least damaging to our system. This is done by balancing the incentives and disincentives in our favor, that is, by increasing the risk of detection and arrest, and concurrently increasing the negative consequences of the illegal act such that the negative consequences far outweigh any positive gain the adversary may envision.

This serious game of balancing incentives and disincentives can be done at many different levels and at many points during an illegal operation. It is appropriate to most potential adversaries except the irrational psychotic.

In the deterrence model, then, the two main variables of concern are the perceived certainty of negative consequences and the perceived severity of negative consequences.

Since the negative consequences of an act of nuclear theft are set by law, or, in the case of an overt attack, are of maximum severity, that is, possible death at the hands of defending security guards, emphasis has been placed on deterrents which impact on the certainty of detection and apprehension.

The probability of detection is increased mainly in two ways: 1) increasing surveillance -- that is, by using more guards, dogs, electronic sensors, informers, intelligence agents, and so forth; and 2) increasing the probability of delay -- that is, by making the criminal act so operationally complicated, cumbersome, or confusing that the authorities will have a better chance of detecting it before it is fully executed.

To these ends, the following general categories of deterrents may be worth considering in a comprehensive deterrence system: first are the pre-event deterrents -- things which may have effect before an actual intrusion is attempted.

Prior to an attempted theft, these deterrents would possibly lower the probability of a successful nuclear theft -- in the case of what we have called "information management," by denying sensitive information and creating uncertainty; and by disseminating limited information about various powerful and sophisticated detection and defense systems which may be in use.

By making it known that intelligence gathering and *infiltration techniques are being* used, it may be possible to increase the perceived probability of detection and to create an atmosphere of suspicion in which conspiracy, collusion, recruitment, and other preparatory actions are more difficult.

By presenting an image of the guard force as being a well-trained, task-oriented team, it may be possible to maximize their presence as a symbolic, personal threat to potential adversaries, and to minimize the perceived chance of gaining inside information through naive members of the guard force.

The second general category is that of the on-site deterrents. On-site, the use of sensory assaults, may cause anxiety, confusion, fatigue, pain, and sensory distortion, and, even if countermeasures are taken, may make it more difficult to mount a well-organized attack.

Various methods of perceptual distortion could be used to cause misjudgments of time, distance, and object and delay the progress of an overt attack.

Symbolic threats such as the presence of random armed patrols, dogs, warning signs, fences, and electro-shock systems could increase fear or anxiety through learned associations.

These on-site deterrents have been the most emphasized category in the project. The reason for this is that, of the various hypothesized deterrents, the on-site deterrents seem to be more reliable and their effects more easily quantifiable. In addition, they fit well into the original FEDS concept. The on-site deterrents are explained in detail in both the preliminary review and in the current update.

Selected on-site deterrents were also discussed at the fourth annual behavioral science symposium and can be found in the proceedings.[3]

The final category is post-event deterrents -- those factors which may lessen the impact of an intrusion and increase the probability of recovering the stolen goods and lead to the apprehension of those responsible for the theft.

The terms, "post-event" and "deterrents" may at first seem to be contradictory terms, but even after the fact, there is the chance that an adversary will abort a theft attempt if the situation is credibly threatening to his goals.

The first post-event problem is to avoid the spread of rumor and exaggerative news reports, and to reassure the public of the capability of responsible police organizations to deal with the theft. In this way it may be possible to deny terrorists their initial goal of inspiring blind fear in the populace. Secondly, through the use of intelligence gathering, the perceived probability of apprehension is increased. And finally, through proper crisis management and contingency planning it may be possible to deny positive reinforcement for planning subsequent acts of nuclear theft.

In summary, the classified and unclassified literature suggest that it may be possible to manipulate several human behavioral processes, but that there are few definitive data directly related to achieving deterrence by means of these psychological manipulations.

[3] Lapinsky, George W.; Ramey-Smith, Ann; Margulis, Stephen T., eds. The role of behavioral science in physical security. Proceedings of the fourth annual symposium, 1979 July 25-26; Nat. Bur. Stand. (U.S.) NBSIR 81-2207(R). 93 p.

DISCUSSION

QUESTION FROM THE FLOOR: In your pre-event analysis, have you given any thought to the impact of the Freedom of Information Act on your selected dissemination of information?

MR. LAPINSKY: No, we have not. The emphasis has been primarily on the on-site deterrents. We included these other aspects because DNA has shown an interest in the broad range of deterrents. In specific applications, we have not looked at the impacts.

QUESTION FROM THE FLOOR: Do psychological profiles differ for each application or do you think they are generally the same?

MR. LAPINSKY: In our analysis of the intruder characteristics, there are a range of threats. Most of the deterrents that we talked about would not be appropriate for the worst case, the terrorist group fully willing to give up their lives, etc. Although the profiles of probable intruders do change with different applications, these deterrents would probably be applicable to all except the worst case.

QUESTION FROM THE FLOOR: I would like to address the previous question about the impact of the Freedom of Information Act and the use of limited dissemination of information. The FAA has had a long-standing program concerning protection of aircraft from bombs, and all of their research and information is excluded from the Freedom of Information Act. It has been extremely effective. There are numerous examples where would-be bombers are simply deterred from carrying explosives on board in the belief that the sophisticated explosive detection system exists.

MR. LAPINSKY: Yes, that is a good point. The deterrence comes with the communication rather than any actual knowledge. And, as long as they perceive a credible risk to their important and relevant goals, there will be deterrence. If it is *not* credibly communicated, there will be no deterrence.

THE UTILIZATION OF EMERGING TECHNOLOGIES IN PHYSICAL SECURITY SYSTEMS

F. A. Bick
Effects Technology, Incorporated
5383 Hollister Ave., Santa Barbara, CA 93111

Dr. F. J. Cook
Adaptronics, Incorporated
1750 Old Meadow Road, McLean, VA 22102

The objective of this program, performed under Contract DNA001-80-C00271, is to investigate the utilization of emerging technologies in physical security systems and to enable a prototype hardware system to be demonstrated for field use. In this first phase, a site security system will be designed and feasibility demonstrated. The emerging technologies that will be used have not been combined in a physical security system before, although each has been investigated in a limited scope.

The proposed system complements ongoing work sponsored by the Defense Nuclear Agency by using three emerging technologies:

Distributed microprocessor data processing
Adaptive Learning Networks (ALN)
Fiber optic data links.

To date, each of these recent technologies has been independently utilized in various applications and each has now reached a level of technological maturity through laboratory and in-service use which makes it possible to use them in conjunction with one another. The result will be a physical security system concept that has capabilities that are potentially much greater than any current system, or any system that might use these technologies independently. Specifically, the benefits that are expected to result include:

Significantly lower false alarm rate

Enhanced probability of detecting intruders

Identification of intruder characteristics

Definition of optimum sensor types and placements

Self calibration for component aging and variations in site characteristics

Greater system and component reliability

Reduced vulnerability to hostile environments, including nuclear

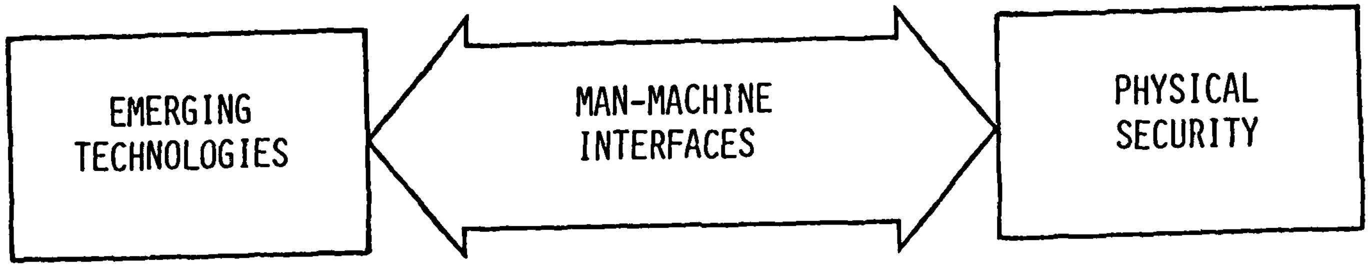
High degree of effective system automation

Effective hardware/security personnel interface (human factors).

These technologies can dramatically affect each of the four basic elements of an effective site security system:

detection and assessment
communication
delay
response

by directly improving capabilities in the first two elements. These improvements will in turn enable more confident use of delay systems and also in utilizing response forces, either on-site or augmentation. This is particularly true through reduction in false alarm rates and more accurate identification of intruder characteristics.



SPONSORED BY: DEFENSE NUCLEAR AGENCY
DNA001-80-C-0271

ROLE OF BEHAVIORAL SCIENCE IN PHYSICAL SECURITY WORKSHOP

11 & 12 JUNE 1980

F. A. BICK
EFFECTS TECHNOLOGY, INC.
SANTA BARBARA, CALIFORNIA

F. J. COOK
ADAPTRONICS, INC.
MCLEAN, VIRGINIA

ETi

PRESENTATION OUTLINE

- EMERGING TECHNOLOGIES
- SYSTEM CONCEPT
- SYSTEM CHARACTERISTICS
- MAN-MACHINE INTERFACE
- CONCLUSIONS

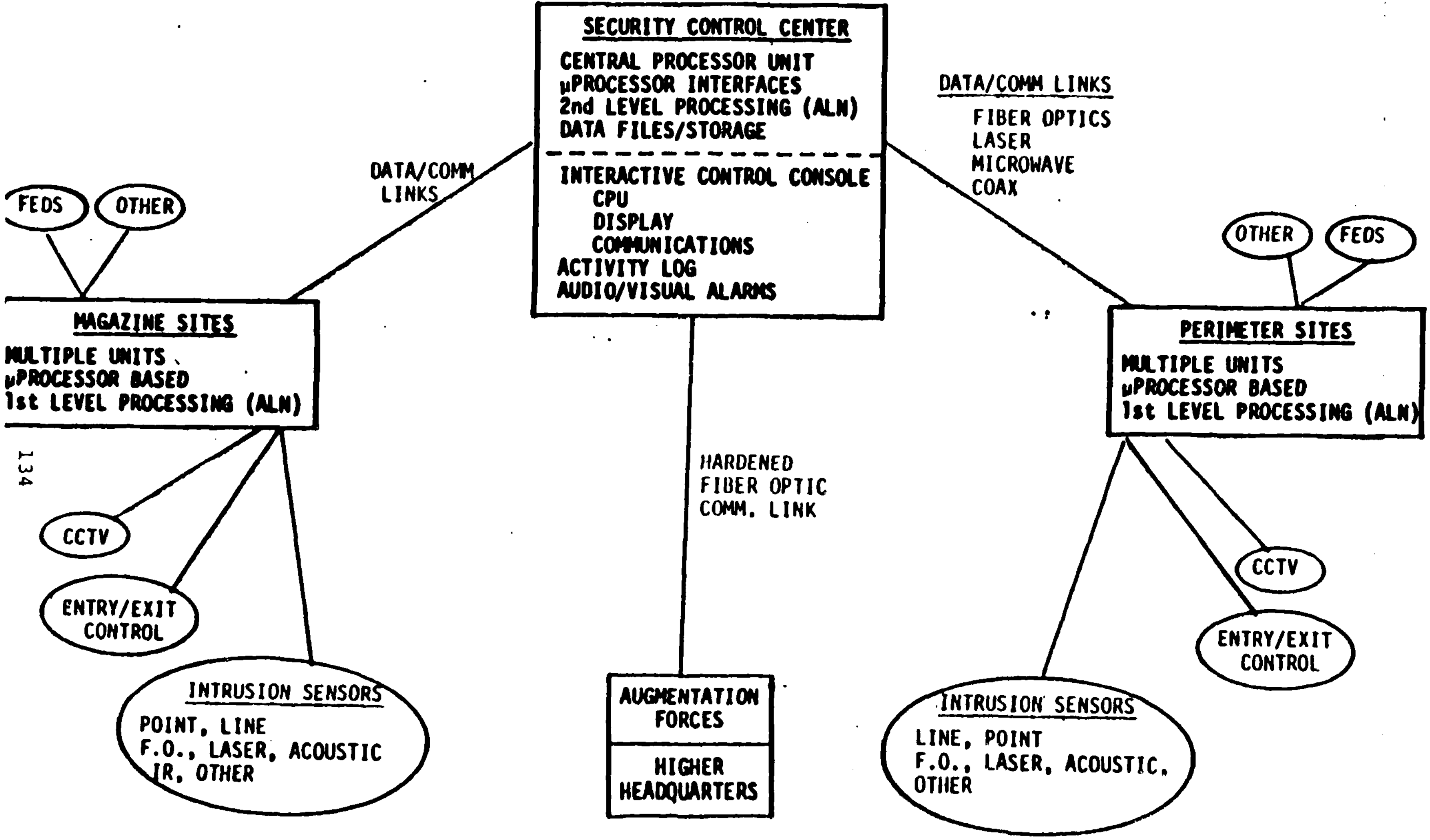
ETI

EMERGING TECHNOLOGIES

- DISTRIBUTED MICROPROCESSORS
- ADAPTIVE LEARNING NETWORKS
- FIBER OPTICS

ETi

SYSTEM CONCEPT (CSSMRS EXTENSION)



SECURITY CONTROL CENTER

CENTRAL PROCESSOR UNIT
μPROCESSOR INTERFACES
2nd LEVEL PROCESSING (ALN)
DATA FILES/STORAGE

INTERACTIVE CONTROL CONSOLE
CPU
DISPLAY
COMMUNICATIONS
ACTIVITY LOG
AUDIO/VISUAL ALARMS

DATA/COMM LINKS

DATA/COMM LINKS

FIBER OPTICS
LASER
MICROWAVE
COAX

MAGAZINE SITES

MULTIPLE UNITS
μPROCESSOR BASED
1st LEVEL PROCESSING (ALN)

FEDS

OTHER

CCTV

ENTRY/EXIT CONTROL

INTRUSION SENSORS

POINT, LINE
F.O., LASER, ACOUSTIC
IR, OTHER

HARDENED FIBER OPTIC COMM. LINK

AUGMENTATION FORCES

HIGHER HEADQUARTERS

PERIMETER SITES

MULTIPLE UNITS
μPROCESSOR BASED
1st LEVEL PROCESSING (ALN)

OTHER

FEDS

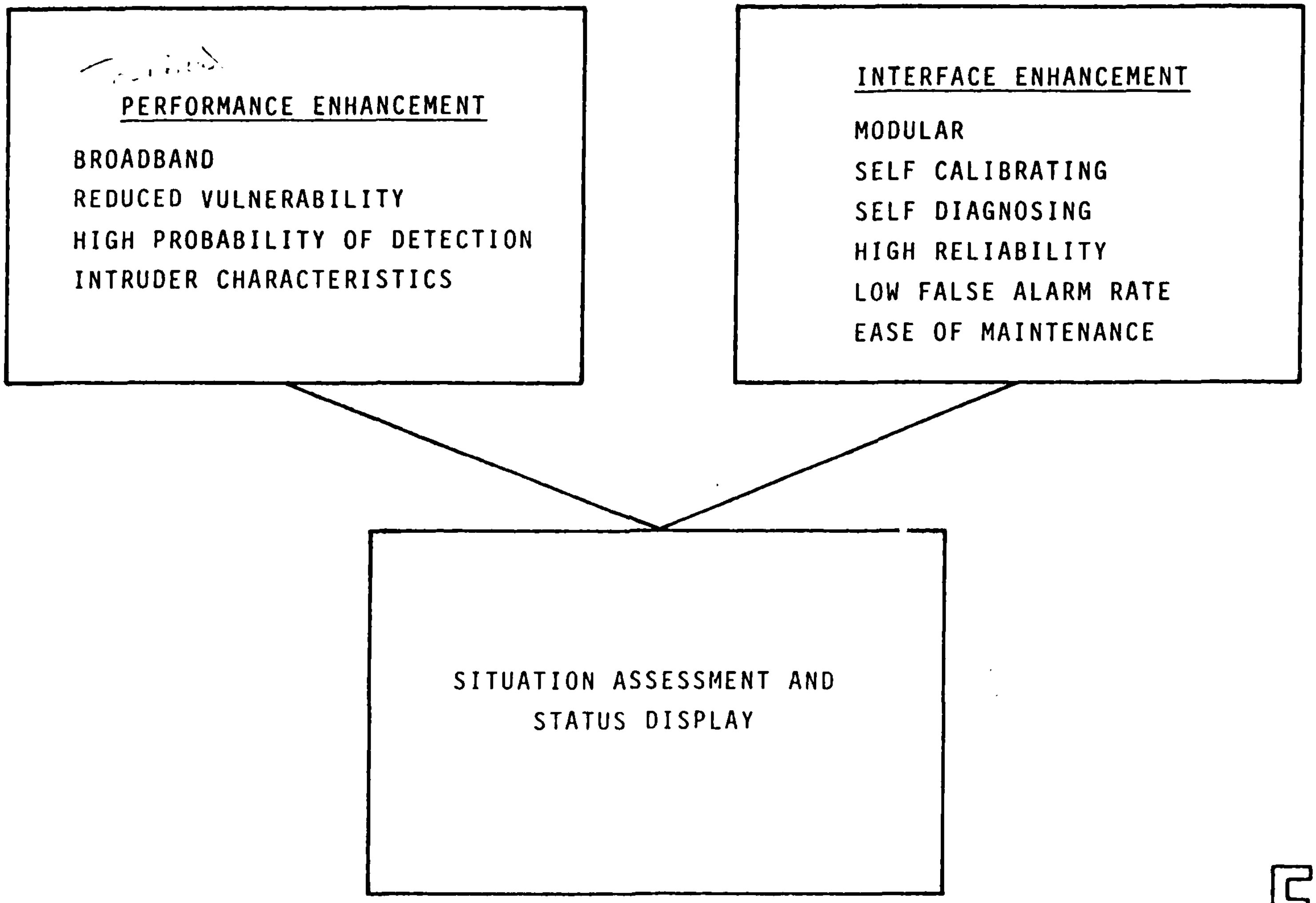
CCTV

ENTRY/EXIT CONTROL

INTRUSION SENSORS

LINE, POINT
F.O., LASER, ACOUSTIC,
OTHER

SYSTEM CHARACTERISTICS



PERFORMANCE ENHANCEMENT

BROADBAND
REDUCED VULNERABILITY
HIGH PROBABILITY OF DETECTION
INTRUDER CHARACTERISTICS

INTERFACE ENHANCEMENT

MODULAR
SELF CALIBRATING
SELF DIAGNOSING
HIGH RELIABILITY
LOW FALSE ALARM RATE
EASE OF MAINTENANCE

SITUATION ASSESSMENT AND
STATUS DISPLAY

ETI

EFFECTIVE MAN-MACHINE INTERFACE

- FORGIVING
- PACED BY OPERATOR
- UNBURDENING
- AMPLIFYING

ETI

EXAMPLE OF AN EFFECTIVE SYSTEM

REMOTE STATION MONITOR AND CONTROL SYSTEM

- COMMERCIAL UNIT FOR BROADCAST INDUSTRY
- MICROPROCESSOR BASED
- CENTRAL STATION MONITORS MULTIPLE CHANNELS/SITES
- PROVEN EFFECTIVE INTERFACES

ETi

PRACTICAL EXAMPLES

SYSTEM APPROACH	QUALITY
SUPPLY COMPLETE SYSTEM	UNBURDENING
SOFTWARE TO CONTROL SYSTEM	UNBURDENING
START SIMPLE AND BUILD FROM FEEDBACK	AMPLIFYING
MINIMIZE RELIANCE ON MANUALS	UNBURDENING, FORGIVING, PACE
AUTOMATE WITHIN LIMITS	UNBURDENING
DOESN'T OVERLOAD USER	UNBURDENING
ALLOW ACCELERATED USAGE	PACE, FORGIVING
SOFTWARE SECURITY	UNBURDENING
PROVIDE STATUS SUMMARIES	UNBURDENING

ETI

CONCLUSIONS

- PROTOTYPE SYSTEM COMPONENTS OFF-THE-SHELF
- SELF-DIAGNOSING AND CALIBRATING
- ADAPT TO SPECIFIC SITE
- LOW FALSE ALARM RATE
- INTERPRET EVENTS AND DISPLAY STATUS EFFECTIVELY
- RELIEVE MAN OF ROUTINE TASKS AND PREVENT OVERLOAD
- DOES NOT ELIMINATE MAN- USES IN MOST EFFECTIVE MANNER

ERGONOMIC DATA BASE FOR PHYSICAL SFCURITY

P. Clare Goodman
Center for Consumer Product Technology
National Bureau of Standards
Washington, D.C. 20234

The National Bureau of Standards has been exploring the possiblity of developing an ergonomics data system since 1976. We summarize some of our preliminary findings and outline our future plans to extend this work to benefit the multidisciplinary field of physical security. First, a brief background of the field of ergonomics will be presented.

"Ergonomics" is the science of applying information about human characteristics to the design of technology. Ergonomic data describes people's capabilities, characteristics, and limitations such as height, strength, and visual sensitivity. An ergonomic data system requires consideration to such factors as:

- Research Planning
- Design
- Development of Standards
- Development of Test Methods, and
- Education.

Many disciplines use ergonomic data, common examples include:

- Human Factor Engineering
- Physical Anthropometry
- Industrial Engineering
- Mechanical Engineering
- Bio-Engineering
- Work Physiology
- Psychology.

The significance of ergonomics is well summarized by Charles Flurscheim (1978), a practicing industrial designer, "Psychological aspects of behavior are becoming more important in their effect on the man-machine interface, for a design that is unsuccessful because of the reactions of the people who use it or will be affected by it is just as unsatisfactory as if it had failed from basic engineering weakness." A common cause of those "people" problems is the phenomena of individual differences. On almost every measure -- from our physical strength to ability to see or learn -- every human is different. Not only are we different from each other, but we differ, over time ourselves, as we are fatigued, injured, etc.

Ergonomic data are usually quantitative and are obtained in controlled laboratory or field conditions. The measurements are obtained from samples of individuals representative of the population that use a piece of equipment or physical system.

To organize the varied types of ergonomic data we can classify them as follows:

- Static Anthropometry,
- Dynamic Anthropometry,
- Strength Characteristics,
- Physiological Characteristics,
- Sensory Characteristics,
- Tolerance to Environments, and
- Reaction Time.

Table 1 lists three of these data classes and then gives examples of the specific ergonomic data that would be needed and some examples of applications.

Table 1. Example applications of ergonomic data.

Area of Need	Specific Ergonomic Data Needed	Data Application
Static anthropometry	Basic human body dimensions as function of age/ sex, etc.	Design of tools and other hard goods, development of clothing sizing and tariffs
Dynamic anthropometry	Bending and stooping capabilities, reach dimensions	Control location and operation, workspace design
Strength characteristics	Static and dynamic force measurements, lifting, pushing, and pulling capabilities	Equipment and job design for industrial workers, product portability design.

Let us briefly describe the current state-of-the-art of ergonomics data collection and usage. An enormous amount of published ergonomic data is available to the person who knows what to look for. Several handbooks are available that summarize much of the data into useful forms for applied problems. These handbook references include:

- Air Force Contractor Design Guides
- Design Data Digest (a digest of military standard 1472B, Human Engineering Guide)
- Human Engineering Guide for Equipment Design (produced through joint funding by the Armed Forces).

These handbooks have several limitations, though, regarding their usefulness in dealing with ergonomic problems. These limitations include the following:

- Difficult to assemble,
- Expensive to update,
- Data are not selectively retrievable,
- Data are in summary form with limited amounts of detail.

Except for these handbooks and some other specialized compilations, systematically developed and evaluated data collections do not exist in ergonomic or behavioral science. In summary, the current state-of-the-art of ergonomic data collection includes such problems as:

- Lack of standard measurement technology
  - Produces inconsistent data
  - Leads to inaccurate data
- Use of specialized populations
  - Prevents data extrapolation
- Existence of obsolete data
- Gaps
  - No longer applicable in important data areas

To improve the situation, the Federal Government has considered developing an ergonomic data base system. The National Bureau of Standards has considered developing a Standard Ergonomic Reference Data System (SERDS) that would provide a single source of critically evaluated, quantitative ergonomic data.

The NBS undertook a user needs survey to answer the following questions:

- How extensive is the need for ergonomic data?
- What specific ergonomic data are most needed?
- Will a data base (such as SERDS) satisfy those specific needs?
- What delivery mechanisms are best?

A sample of approximately 4400 persons of anticipated users was identified by randomly selecting names from professional organizations concerned with ergonomic data. For example, such diverse groups as:

- o American Psychological Association
- o Human Factors Society
- o Industrial Design Society
- o Standards Engineers Society
- o Acoustical Society of America
- o American Society for Testing and Materials
- o American Society of Heati'g, Refrigeration and Air Conditioning Engineers
- o American Apparel Manufacturers Association

The survey was divided into four sections with each addressing a separate set of questions.

Section 1 covered demographic characteristics of the respondents. Section 2 and 3 requested detailed responses about specific types of ergonomic data to be included.

Specifically, the second section intended to provide insights into the frequency of use and the satisfaction with present formats for ergonomic information. The third section provided information as to how frequently respondents use ergonomic data for each of the eight population groups, and how adequate the existing ergonomic data are for selected categories.

The final section covered the perceived impact of SERDS to the respondents employer and profession.

In this presentation, are summarized the preliminary findings of 46 respondents who were from the DoD agencies. One must remember that these 46 responses do not represent the over 1000 responses received, nor do they represent the entire population of DoD personnel who use ergonomic data. The results from the 46 respondents can only be used as a rough guide.

RESULTS

Most respondents were trained in psychology or engineering. Seventeen respondents were affiliated with the Army, 14 with the Navy, and 10 with the Air Force. The remaining five were employed by various other organizations with DoD. The respondents were requested to indicate their primary duties. Applied research, R&D management, and consulting involved a large part of the sample.

The frequency of use and relative satisfaction with presently available ergonomic data references were rated by the survey respondents. As shown in table 2, the most used sources of ergonomic data (used occasionally-to-often) are military standards.

Table 2. The frequency of use and relative satisfaction of presently available ergonomic data references.

Frequency	Data source	Number sometimes to usually satisfied	Number rarely satisfied
38	Military standards	36	2
35	Personal contact	35	0
35	Handbooks/guides	32	3
33	Separately published reports	32	1
30	Journals	27	3
25	Ergonomic textbooks	23	2
25	ISO... standards	22	3
22	Non-military standards	19	3
19	Computer data base	19	0
13	Outside expert	13	0

Thirty-six respondents were usually or sometimes satisfied with ergonomic data contained in military standards, with only two rarely satisfied. Users were somewhat less satisfied with ISO, ASTM or similar ergonomic standards and with non-military government standards, but, even for these sources, 22 were sometimes-to-usually satisfied.

Fewer respondents made use of computer base ergonomic data or outside ergonomic experts, but those who did were always sometimes-to-usually satisfied.

In response to the question: "Does your employer perform or commission empirical ergonomic/human factors research?", 35 respondents indicated that such research is done for their employers. More than half of these respondents noted that empirical research was done because necessary ergonomic data do not exist or are based on non-representative samples.

Eight population groups are listed on the survey form, but only three are considered relevant for DoD/military applications. They are:

- General Population (13-65 yrs. of age)
- Military Personnel
- Ethnic/Racial Groups.

Generally, most responses were concerned with the military personnel population group. Only one-quarter of the respondents indicated they were concerned with questions involving ergonomic data for ethnic/racial groups.

Questions were asked to determine how frequently the respondents used data for each population group, as well as the adequacy of the data for each population group. The ergonomic data were divided into the following 11 broad categories:

- Static anthropometry
- Dynamic anthropometry biomechanics
- Strength
- Physiological processes
- Auditory processes
- Visual processes
- Tactile sense
- Psychomotor processes
- Tolerance to environment
- Learning and memory processes, and
- Stereotypical behavior.

The respondents indicated they needed ergonomic data on the general population as well as for military personnel in order to perform their jobs. For the military personnel population, the most often used ergonomic data categories were psychomotor and visual pıocesses. The data categories with the greatest number of rarely satisfied users are: tolerance to the environment; psychomotor processes; learning and memory processes; and stereotypical responses.

Next, these preliminary results are highlighted, but once again the reader is reminded that they represent only 46 data points.

- Military users of ergonomic data need information about populations other than military personnel.

- Generally, military standards are the most used reference source, followed by personal contacts, handbooks and guides. Few users were "rarely satisfied" with the most used ergonomic data sources.

- Most users were "sometimes" to "usually" satisfied with most of the types of ergonomic data asked about. For example, static anthropometric data for military and general populations were considered satisfactory by most: fewer users were satisfied with such data broken down for ethnic/racial groups.

- Tolerance to the environment and stereotypical responses were areas where many users were "rarely" satisfied with available ergonomic data.

- Users prefer statistical summaries and considered hard copy the most useful output and raw data and computer tapes as the least useful.

When asked specifically if SERDS would help to improve profitability or reduce costs for their employer, 24 said yes, 2 said no, and 15 indicated they did not know.

A DoD ergonomic data base would supply critically evaluated, quantitative data related to human factors essential for the design, operation and maintenance of complex and sophisticated physical security systems for nuclear and non-nuclear applications. For example, included would be ergonomic data that directly influence the design of control monitoring rooms. Proper design of control monitoring rooms based on knowledge of the human characteristics, capabilities, and limitations of security personnel should enhance physical security and increase morale.

In addition to supplying quantitative data a system would: describing would:

- Provide a single source for information,
- Include only screened information,
- Reveal gaps in information,
- Reduce research costs, and
- Reduce search time.

During the remainder of 1980, NBS will prepare a more detailed user needs survey for DoD ergonomic data users to examine the requirements for an ergonomic data base on physical security. The survey will be designed to:

1. Identify the types of ergonomic data now available for DoD physical security application.
2. Determine the level of satisfication with available ergonomic data.
3. Identify what specific ergonomic data are most needed.
4. Establish priorities for ergonomic data.
5. Determine if an ergonomic data base would satisfy DoD physical security needs.

In 1981, NBS plans to distribute the survey to a statistically representative sample of DoD ergonomic data users and analyze the results.

Editors Note:

The military survey questionnaire described in this paper was prepared and submitted to DNA in 1981 for use by DNA rather than NBS, as a consequence of eliminating behavioral science activities from the scope of the LESL activity.

THE EFFECTS OF WEATHER SENSITIVITY ON STRESSED PERSONNEL

DR. CHARLES WALLACH

Decisions and Designs, Inc.
8400 Westpark Drive
McLean, VA 22101

INTRODUCTION

Over the past decade or so the discipline of Behavioral Science has grown to include the study of biochemical effects on human behavior. In earlier days, behaviorists concerned themselves mostly with learning and conditioning phenomena, with motivation and attitude modification, and other forms of applied psychology that operated above eyebrow level. Now we are rapidly breaking new ground in the field of psychophysiology, in establishing mind/body interactions, and in developing an understanding of the important role of biochemistry in controlling brain activity--even at the level of emotional and social behavior.

Substantial impetus toward this new frontier was generated by the pioneering work of Dr. Albert P. Krueger, of the University of California, in finding a link between the electrical qualities of environmental air and blood serum levels of serotonin--a potent neurotransmitter hormone which has been closely associated with stress.

Others who follow him have succeeded in relating the balance of airborne electrical charges (ions) to the production or inhibition of other hormones, or biochemical families, and in tracing the effects of these relationships in influencing human behavior over a surprisingly broad range of emotional manifestations and physiological metabolisms.

These studies, together with the rapid advance in the technology of bioassay which enable us to objectively prove many of the links between the external environment and the internal biochemical balances, are being extended to the discovery of other environmental affectors which impact on human mind/body interactions, behavior and metabolisms.

We are now engaged in exploring the effects on behavior of such environmental factors as light, color, energy fields (sferics) and sound. And we are finding that a great many behavioral phenomena which were formerly thought to be generated above eyebrow level, are actually triggered by sensory and subsensory stimuli from the external environment.

This new class of subtle, external triggers is called "Microbiological Environmental Affectors" (MEA's), to distinguish them from primary chemical allergens--although the two groups often have similar effects. One of these MEA's is the atmospheric ion factor, the effects of which were first observed in the context of human weather sensitivity; and the purpose of this paper is to describe how this particular factor may relate to the human factors and ergonomics of physical security.

WEATHER SENSITIVITY AND STRESS

Considering for the moment only the ion factor, biometeorological studies indicate that about a third of any large population sample may be found "weather sensitive" to an easily measurable degree, and another third at a more subliminal level. This sensitivity is even further heightened in individuals by the presence of other forms of physical or psychological stresses which alter the normal, baseline balances of biochemical groups.

At the present state of the art of bioassay, the four biochemical groups among which such variations can be measured among the more sensitive fraction of the population are:

serotonin/endorphin - related to stress and pain;

catecholamines - related to fatigue and alertness;

thyroid factions - may relate to mental stability.

These indicated relationships are really gross oversimplifications, but may serve our immediate purpose and avoid boring you with technicalities. Also, there is a wide variation among individuals in the degree to which any one of these groups is affected; that is to say, it is most unlikely that anyone would experience irritability, fatigue, breathlessness and a touch of paranoia all at the same time, under depressive atmospheric conditions.

In analyzing the biodynamics of these effects, weather-change vectors were identified as:

temperature,

humidity,

atmospheric pressure,

electrostatic field gradients,

+/- gaseous ion balance.

But experimental evidence indicates that within its normal range of meteorological excursions, each of these vectors can be eliminated as the basic cause of such biochemical shifts except the ion balance factor.

Among those individuals who exhibit observable forms of weather sensitivity--or perhaps we can call this "ion sensitivity"--under suboptimum ion balance conditions, nearly half (44%) show serotonin-related symptoms dominantly, and a like proportion experience catecholamine-related symptoms. Only about 13% show signs of interference with thyroid metabolism resulting in irrational behavior, and this usually develops only after several hours in the depressive atmospheric environment when other stresses are present. In addition to these specific effects, there is evidence of an overriding prostaglandin disbalance (related to blood circulation and respiration problems) which may affect a large but undetermined fraction.

ION DYNAMICS

There are, of course, many kinds of ions in solids, liquids and gasses; for our purpose we will consider only the class of monomolecular, gaseous ions which interact electrically at the surface of living tissue. In this context, a negative ion is a neutral molecule (usually $O_{\bar{2}}$) which has captured an extra free electron and is attracted to any other molecule or surface with a more positive charge, where it delivers over its extra electron and becomes neutral again.

Conversely, a positive ion is a molecule which has had one of its normal complement of electrons knocked away by some nearby, random, subatomic event; then it is attracted toward any more negatively charged surface where it can easily replace its missing electron at a low energy level.

Both positive and negative ions are being created continuously by the various forces of nature, but they are usually short-lived because they are continuously being reneutralized by this process of electron change.

Let's assume, for example, that during one inspiration a million negative ions enter the respiratory system, and each one delivers up its extra electron to the surface tissues of the bronchi and lungs. These million newly liberated electrons would tend to travel *into* the deeper tissues of the body in the form of a disperse current flow. This would tend to affect the electrical fields of cells involved in the manufacture of biochemicals and to influence the metabolism of these biochemicals.

I say "tend to" because during the same inspiration, perhaps a million positive ions also enter the respiratory system, and each of these borrows an electron from the tissue surface it encounters. These electrons would be replaced at the surface from deeper tissues and tend to start a disperse current flow *out of* the body; but in this case, where the effects of the positive and negative ions are equal and opposite, the net current flow would be zero.

So it is only when there is a prepondernace of either positive or negative ions that this electron-exchange phenomenon results in electrochemical effects in the deeper tissues, and so alters the orchestration of our complex biochemical systems.

In fresh, outside air during fair weather, there are roughly equal concentrations of +/- ions; we consider this as normal, or baseline, ion balance. However, preceding every storm (sometimes by as much as a day or two, depending on the severity of the storm) there is a substantial-to-massive increase in the concentration of positive ions, which has a "negative" effect on ion-sensitive people. This is why some folks become irritable, dull-witted, less productive, depressed or more sensitive to pain under prestorm conditions, especially when they are supporting other forms of stress.

After the storm, this air-ion disbalance is quickly reversed, and there is an overabundance of negative ions. This not only relieves the symptoms of positive-ion depression, but often produces euphoria, heightened vitality, alertness, enhanced sensory acuity and--if we can extrapolate the observations of animal breeders--heightened sexual drive.

Knowing this, a field commander might achieve a slight tactical edge by artificially charging his personnel with negative ions and attacking the enemy just before a major storm, given a good meteorologist on his staff.

But weather effects are transitory and seldom comform to the order of battle, although it might be useful to keep them in mind when major storms are in the offing. What is of significance here, however, is that we are just beginning to recognize the fact that with our modern, efficient architecture, we are creating artificial working environments in which we have very often *simulated* the most severe prestorm, high-positive-ion conditions, to the serious detriment of a certain number of our personnel working under stressful conditions which inevitably are situations requiring very high levels of vigilance, sensory acuity and fast reaction time or, for that matter, the exercise of high levels of intelligence in planning and command tasks.

CONTINUOUS PRESTORM IONIZATION CONDITIONS CREATED IN MAN-MADE STRUCTURES

The architecture of watchowers, interior guard posts[1], control[2] and communications rooms[3] is generally highly space-efficient, particularly in windowless, hardened sites. This is also true of patrol vehicles and armor[4]. These environments always include some combination of other factors, each of which contributes either to the reduction of negative ions, the increase of positive ions, or both. The magnitude of the resulting shift in ion balance often greatly exceeds that of natural, prestorm conditions, to the point where measurable performance degradation can be observed among personnel working in such environments for hours at a time.

Some of the factors which contribute to this effect are:

inadequate window area or very thick windows;

forced-air circulation through ducts;

wind friction on external building (or vehicle) surfaces;

air-conditioning and filtering equipment;

fluorescent lighting fixtures;

low ceilings (8' or under);

electrical equipment (radios, displays, typewriters);

synthetic floor surfaces and ceiling materials;

tobacco smoke;

large metal furniture (cabinets, safes, desks, etc.)

Numerous measurements made with laboratory instrumentation in such typical environments, and also in closed vehicles, provide objective evidence of massive ion-balance deficiencies and support the subjective reports of personnel working therein. For example--and this is only one of many instances--in the Spring of 1978 I was invited to make ion measurements in the Defense Nuclear Agency office suite occupied by Marvin Beasley's officers and colleagues.

At 2:10 p.m., immediately prior to these tests, measurements were made in the fresh, outside air in a shady area on the lawn outside the DNA Headquarters; we found a positive ion count of 1,110 ions per cubic centimeter of air, and a negative count of 960/cc. This indicated a +/- ratio of 1.16:1, which is quite normal for fair weather conditions in a rural environment, and a total ion count of 2,070/cc (a parameter which is of long-term biological significance).[5] At about 2:20 p.m., in the testing area, we measured about +80/16, or a ratio of 5:1 and a total of 96 ions/cc, or about 6% of an acceptable, healthful level. In fact it was difficult to determine values accurately so low on the scalar levels of the instruments.

After taking these measurements, I interviewed the personnel and learned that about half of them were aware of becoming progressively more inefficient and dull-witted towards the end of the day; this was particularly true of the nonsmokers affected by the heavy output of tobacco smoke without benefitting from the stimulation of the nicotine, and it was also noted that the coffee consumption of this group was unusually high with respect to the norm among personnel on other floors of the building with well-windowed and more spacious offices.

Apart from the professional and scientific interest of these officers and civilians, another purpose of this test was to evaluate the need for the installation of electronic negative ion generators, to restore a more natural ion balance and increase the very low total-ion count. Two such devices were subsequently tested on a loan basis, and the observed environmental improvement was determined to justify procurement requisitions which were submitted in due course. Unfortunately for these personnel, however, acquisition was vetoed by someone sitting in a spacious, airy office upstairs.

This brings up the point that not everyone is aware of being affected by unnatural ionic conditions, probably be use their autonomic biochemical control systems are capable of compensating for these effects. So it is understandable that people not continuously subjected to poor ionic environments, and also ion-insensitive individuals usually find it difficult to sympathize with the sensitives, or to accept the fact that such effects exist. There appears to be a genetic factor involved in ion-sensitivity, which is often reflected in body type and evidenced in sustained levels of task performance or work output.

A typically ion-insensitive individual is characteristically found to have a sturdy skeletal structure and body-build, and a brachycephalic skull configuration. Marv Beasley, whom we all know, is an excellent example; he is also capable of working effectively in that difficult office environment for hours after his colleagues have left in a miasma of fatigue. Although apparently insensitive to ion balance effects himself, it is a tribute to his keen perception that he recognizes such effects may occur among the tall, thin, narrow-headed or corpulent body-types among which ion sensitivity appears to be common. I trust he will forgive me for using him as an example in the interests of behavioral science, of which he has always been a strong proponent.

ION SENSITIVITY COUNTERMEASURES

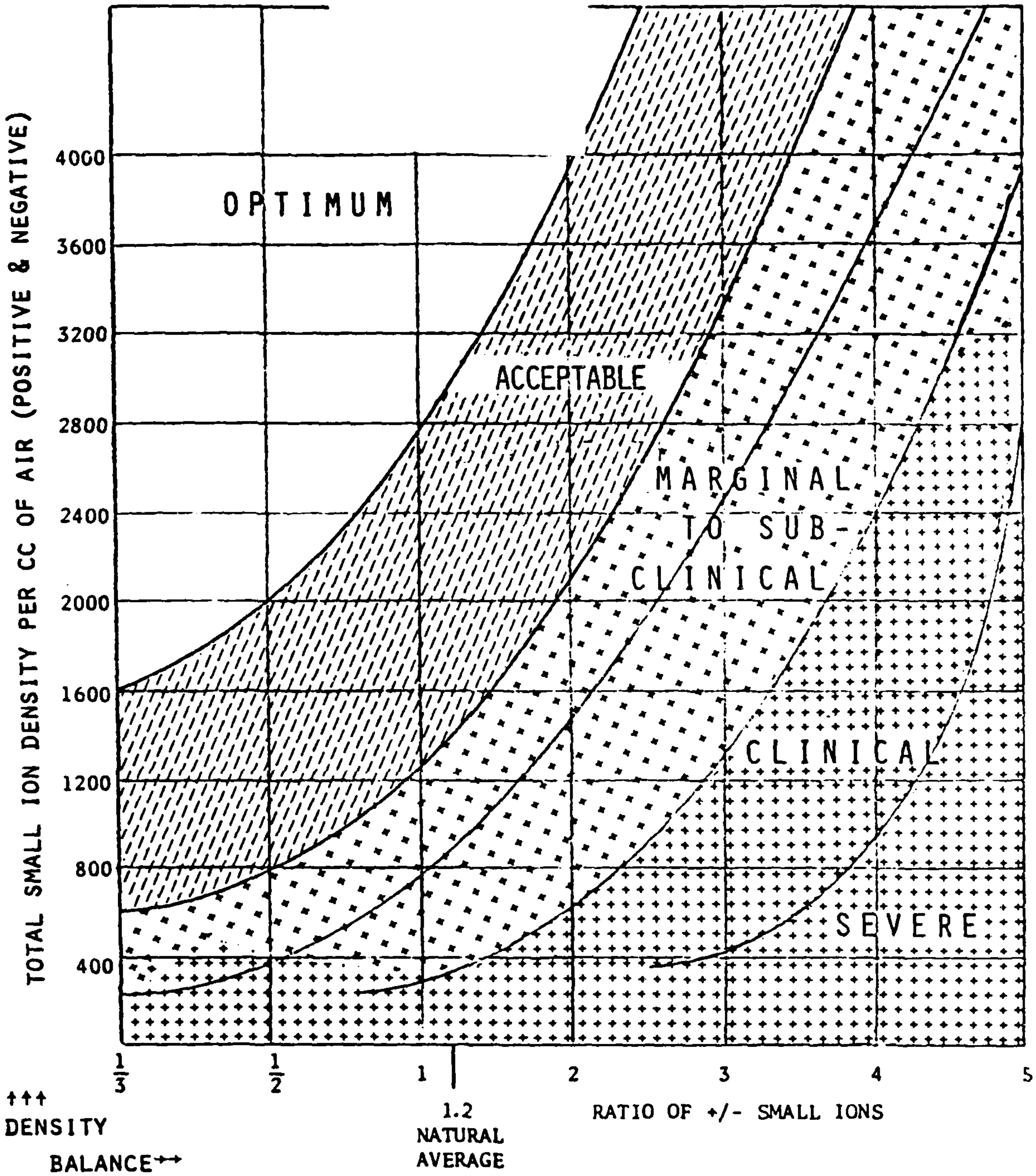
Where deviations from acceptable ion densities and/or balances are observed to exist in working environments, they can be countered effectively and economically by the installation of suitable electronic devices which create negative ions to offset high attrition rates in poor ionic environments. Concurrently with the spread of information on the biological effects of air-ion balance in journalistic media, there has been a proliferation of poorly designed ion-generation systems brought into the market; these have been responsible for enough disappointing experiences among the nontechnical public to somewhat slow general acceptance of the technology. But high-quality, professional devices are available for these applications at a cost of $1 or less per square foot of working space coverage.[6]

Negative ion concentrations produced by these devices vary geometrically with distance from the source and are also affected by local air currents; but quantitative measurements are not critical to the application within their effective range of six to ten feet, as there are no harmful side-effects from large concentrations of negative ions[7] -- which often achieve 20 to 40 times baseline levels under natural conditions at seashore sites, in pine forests or nearby waterfalls.

Figure 1 is a matrix of weighted values compiled from the medical literature and may serve as a useful guide to acceptable levels in working, standby and living environments.

In the profession of physical security and safeguards, it is not possible to quantify the value of human performance quality; a small increment of degradation may be analagous to the proverbial horseshoe nail that lost the Battle of Hastings. To lend some perspective, let's assume that one quarter of a given guard force is made up of ion-sensitive individuals, and that under adverse weather or ion-environmental conditions we can measure an average of 20% vigilance degradation; these figures are very conservative with respect to actual field observations.

This represents an overall 5% reduction in force effectiveness which, if sustained over long periods, begins to impact on that subtle factor of motivation but may not



ESTIMATED ION DENSITY/BALANCE BOUNDARIES
OF EFFECTS ON 30% (-4 to -1 S.D.) OF ANY
LARGE GENERAL GROUP AFTER 4 HRS EXPOSURE

FIGURE 1

N.B. TOTAL ION DENSITY RELATES TO LONG-TERM METABOLIC EFFECTS SUCH AS SODIUM/POTASSIUM LEVELS. +/- BALANCE RELATES TO SHORT-TERM BIOCHEMICAL EFFECTS MORE RELEVANT TO THE EFFECTS DISCUSSED IN THIS PAPER.

otherwise look like a major threat. On the other hand, in Don Richard's scenario with the fishpole, the sensitive group *on the average* might start ignoring a signal after the fourth false alarm instead of after the fifth; again, this may not seem of great importance. But consider the one or two individuals in this sensitive group at the extreme of the sensitivity range (S.D. = 8%) whose performance may be degraded by 50% or 60%; these are the ones whose performance profile will reveal the greatest vulnerability; they're the ones who are most apt to go off half-cocked and fire the unnecessary shot that starts the war.

Of course these highly ion-sensitive individuals should never have been assigned to such critical duties in the first place, which brings us to the excellent arguments advanced by Clare Goodman for the development of an ergonomics data system to meet the requirements of personnel selection in physical security tasking. Gross probability of individual ion balance susceptibility should not be difficult to evaluate, and there appears to be good justification for using this parameter in the selection process. Early fatigue is another dominant characteristic of ion sensitivity (43% incidence of the catecholamine syndrome), and Larry Ewing's remarks about fatigue in his shipboard behavioral model offer additional justification for ergonomic measurements of ion sensitivity, particularly as this is closely related to stress-level by virtue of the serotonin connection.

It may be some time before we arrive at the point where we can eliminate hypersensitive and hyperstressed personnel from critical task assignments under potentially suboptimum ionic conditions; in the meantime, there are electronic devices and systems available to improve the quality of such environments and lessen the constant threat of human fallibility in critical security tasks. Some immediate applications of these devices which may be of interest to this symposium are:

GUARD POSTS - to enhance vigilance[1|2|8] and sensory acuity[9]

PATROL VEHICLES - to minimize reaction time[4]

CRISIS CENTERS - alertness; minimizes brain-fog and fatigue of sustained tension (and tobacco smoke fog)

DEĆONTAMINATION - rapid precipitation of airborne particles[10] and acceleration of lung clearance through biological action (radioactive particles)

WOUNDS - reduces trauma shock and accelerates recovery from blood loss[11]

DETENTION FACILITIES - reduces stress-induced
disciplinary problems
and the spread of air-
borne respiratory diseases

It is noted parenthetically that Daryl Solomonson's investigation of behavior in watchtowers revealed a common syndrome of troublesome discomfort and nausea in windy weather; this is attributed to tower sway by association rather than through any objective evidence. In fact, the friction of wind on the metal housing imparts a positive electrostatic charge which, inside the enclosure, quickly attracts and depletes the negative ion population. This is the same phenomenon that occurs in moving vehicles, and accounts for a large fraction of motion sickness problems. Many such sufferers have found that the use of a small generator to replace the depleted negative ions will prevent the onset or relieve the severity of these symptoms. I do not suppose, however, that this would be helpful in nausea induced by vertigo, which involves a different set of neurophysiological dynamics.

NEAR-TERM RESEARCH OPPORTUNITIES

Our analysis of the literature indicates that up to 20% of a healthy, military force may be transiently affected by ion shifts up to 48 hours prior to and during storms and sustained high winds. The specific effects involves degradation of vigilance, sensory acuity, reaction time, mental alterness and stamina. The personnel screening and selection process for assignments requiring optimum performance in these behavioral areas does not now include accessable physical parameters of weather sensitivity because these have not been adequately evaluated and defined. Some promising starts have been made in this direction, which indicate potentially useful approaches to the rapid development of suitable ergonomic standards if this effort is given appropriate support.

More significantly, up to 65% of the personnel working and/or living in enclosed artificial environments (buildings or vehicles) under poor ionic conditions probably experience similar performance degradations which increase at varying rates with exposure duration. As ergonomic screening of such a large group would not be feasible, the more practical and economical alternative of artificially restoring normal ion balances is the indicated countermeasure. Our research targets whould therefore include:

1. evaluation of +/- ion ratio thresholds to establish boundary conditions and acceptable exposure intervals;

2. quantitative analysis of effects and susceptibility index of typical populations;

3. development of architectural standards to minimize deleterious ion balance conditions;

4. application engineering standards for determining specific space requirements for negative ion generation equipment;

5. ion generator equipment design and performance specifications for (a) preliminary research efforts, and (b) field use.

These are not listed by priority, as there is some interdependence among these efforts and the different disciplines involved.

Decisions and Designs, Inc. (DDI) is currently tasked by DNA to explore the application of ion technology in the intrusion-detection modality, as some of these devices have proven to be highly effective sensors in this application. This development will be reported elsewhere, as it does not relate to behavioral science; however, in the performance of these task requirements, DDI has developed an exceptionally fine air-ion measurements laboratory and an extensive background in the basic physics and technology of ion generation. It is hoped that organizations investigating the biological effects of air-ion balance and density will be able to make effective use of this resource.

THE SHAPE OF THE FUTURE

In discussing the effects of weather and ion sensitivity on stressed personnel, we are focussing only on the transient effects of a single facet of Microbiological Environmental Affects (MEA's) mentioned in my introductory remarks. There are a number of other significant MEA's--light spectra, sound, olfaction, energy fields (sferics)--which impact upon the human biochemical systems in varying, individualistic degrees, to shape behavior. Under modern environmental conditions where these effects are sustained more *continuously*, rather than peculiar to a short-term working environment, they may bring about long-term cumulative behavioral changes which begin to affect social structures when a large enough fraction of the population is involved.

This is precisely the case where both working and living environments in modern, urban and suburban or institutional settings are suboptimum or worse with respect to MEA factors.

As new population groups undergo a transition from their accustomed, traditional, rural living environments to life in crowded, noisy poorly ventilated and ill-illuminated quarters in urban, inner-city or fringe-area slums, much high incidence of MEA-sensitivity will be found among these unhabituated groups. In terms of social stresses and behavioral patterns, this impacts particularly on the younger population in growth and maturation stages. Such groups may require a generation or more to adapt to the biochemical shifts triggered by the MEA's of new environments, and the resulting psychological stresses may be evidenced in ways which become statistically apparent to the social scientist.

For example, at least some part of the ineluctably rising crime rate among the 14-34 year segment of inner-city populations in this country could conceivably be linked to lack of adaptation to stress-inducing MEA's. Similarly, the progressive increase in terrorism observed in emerging countries, where urbanization is proceeding rapidly among low-income, pastoral populations, could conceivably be linked to novel environmental factors.

This suggests the possibility that there may be a *biological* factor involved in the rise of crime and terrorism, which is being manifested as heightened social stresses among a portion of the younger generations.

Evidence at hand is sufficient to warrant investigation of this possibility on a broad, multidisciplinary scale, in the interests of shaping peaceful, productive societies. It is in areas such as this that behavioral science may have substantial contributions to make in shaping the future.

1220 Blair Mill Road
Silver Spring, MD 20910

12 June 1980

BIBLIOGRAPHY

1. Effects of Air Ionization upon the Performance of a Vigilance Task, *Halcomb, C. G. and Kirk, R. E.*
1965, J. Engineering Psychology, v4/4, pp 120-126.

2. Air Ions In Physical Medicine and Environmental Engineers, *Laws, C. A., Holiday, E. R.*
January 1975.

3. Communications Room Ambiance, *Wallach, C.*
1979, IACP Equipment Technology Center, Bulletin 79-4.

4. New Police Car Safety Development, *Wallach, C.*
1979, IACP Equipment Technology Center, Bulletin 79-3.

5. Influence of Ionization on Endocrine Glands, *Gualtierotti, R.*
BIOCLIMATOLOGY, BIOMETEOROLOGY AND AEROIONOTHERAPY,
1968, Carlo Erba Foundation, Milan, 167 pp, illus., $22.

6. UPDATING THE ION CONTROVERSY, *Wallach, C.*
1979, Int'l Bio-Environmental Foundation, MD 20910,
98 pp, $6.50.

7. Absence of Harmful Effects of Protracted Negative Air Ionization, *Sulman, F. G. et al.*
1978, Int'l J. Biometeorology, v22/1, pp 53-58.

8. Air Ions and Human Performance, *Hawkins, L. G. and Barker, T.*
1978, Ergonomics, v21/4, pp 273-278.

9. The Effects of Atmospheric Ions on Visual Parameters, *Mizusawa, K.*
1969, Proc. SPIE Space Optics Seminar, v19, pp 23-26.

10. Air Ionization: A Possible Method in Controlling Air Contamination, *Makela, P. et al.*
1978, Proc. 4th Int'l Symposium on Contamination Control.

11. Effect of Inhalations of Air Ions on the Electro-Chemical Properties of Blood during Exsanguination and Recovery of Cats, *Kusmina, T. R.*
1967, Int'l J. Biometeorology, v11/2, pp 191-194.

1980 Carnahan Conference on Crime Countermeasures
University of Kentucky, Lexington, Kentucky – May 14-16, 1980

FACILITY INTRUSION DETECTION SYSTEM

by

Ben Barker
U.S. Army MERADCOM

and

R.A. Miller
GTE Sylvania

Abstract. The Facility Intrusion Detection System will provide physical security protection for Department of Defense (DOD) facilities containing sensitive items that may be prime targets of organized criminal elements, insurgent organizations, espionage, or sabotage groups. A variety of sensor devices report intrusion conditions at remote areas to a monitor console via a secure data link. The protected areas may be the interior of structures or the exterior area surrounding these structures. Audio and/or video surveillance of an area can be performed at the command console upon receipt of an intrusion alarm. Activation of deterrent devices can be initiated by command from the console when an intrusion is verified thru surveillance. Deterrent devices will delay the intruder in the accomplishment of his mission thus providing more time for response forces to intercept the intruders and deny intruder access to equipment or material which could be used by terrorist groups to threaten the response force of the local populace. The system provides flexibility for use in different types of areas as a result of the variety of sensor types available, and the capability to provide a variable system (command and control) configuration.

The sensors for interior applications include such types as vibration, ultrasonic motion, passive ultrasonic, passive infrared motion, duress, balanced magnetic switch and capacitance proximity. Controlled and/or commandable devices in the remote area include entry control devices, audio surveillance microphones, voice communication devices, deterrent devices, video surveillance devices and special function devices.

General Overview

The Department of Defense is expending considerable effort to develop physical security equipment which can be effectively integrated into security systems for critical DoD facilities. To ensure that equipment development by each of the military services can be easily integrated, a Security Equipment Integration Working Group (SEIWG) has been chartered by the Office of Undersecretary of Defense for Research and Engineering (OUSDR&E), Physical Security Equipment Action Group (PSEAG). The SEIWG meets at least once each quarter to consider both equipment and system interfaces. Chairmanship of the SEIWG rotates among the military services with representatives of each of the service sensor system developers actively participating. This representation includes personnel from the U.S. Army Mobility Equipment Research and Development Command (MERADCOM) at Fort Belvoir, Virginia for the Facility Intrusion Detection System (FIDS), the U.S. Army Electronics Research and Development Command (ERADCOM) at Fort Monmouth, New Jersey for the Remotely Monitored Battlefield Sensor System (REMBASS) and the U.S. Air Force Physical Security Systems Directorate (PSSD) at Hanscom Air Force Base for the Base and Installation Security System (BISS). The subject of this paper is the design of the FIDS which will be a key part of DoD's Land Based Physical Security System.

The purpose of an intrusion detection system is to monitor as depicted in Figure 1 and report the entry (authorized and/or unauthorized) into an area. Area's within DoD that are deemed appropriate for an intrusion detection system include:

Weapons Storage Facilities
Nuclear Facilities
Strategic Weapons Sites
Computer Centers
Document Data Centers
Chemical Storage Facilities

These intrusion detection systems, also referred to as physical security systems, are comprised of major groups of equipment consisting of sensing devices, communications links, and monitor/display hardware. Each system configuration varies in size and complexity and is totally dependent on the particular application. This dependency on the specific application often times created difficulties or even impossibilities for the available equipment groups to satisfy the requirements levied on a specific intrusion detection system implementation. Much of this lack of equipment flexibility and/or expansion capability was due to equipment design that is totally hardware dependent thereby requiring extensive hardware changes to meet a specific intrusion detection

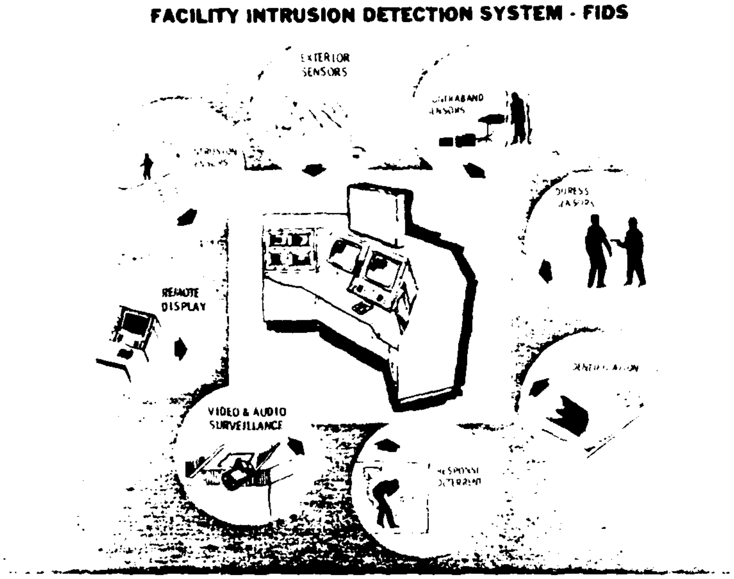


Figure 1. FIDS Monitor Techniques

system requirement. With the advent of the microprocessor and supporting electronics the flexibility of equipment applications through software changes has provided a new dimension to intrusion detection system.

The Facility Intrusion Detection System (FIDS), utilizes the microprocessor technology, to the fullest extent, thereby providing a system with the flexibility necessary to satisfy the broadest of security system applications known today. FIDS shown in simplified block diagram form in Figure 2 provides the capability to monitor, command and control any number of remote areas from one to 2048. A single remote area can be configured with up to 48 intrusion detection sensors, an entry control device, and several commandable devices all interfaced to a single control unit (CU) located in the remote area. The heart of the CU is a microprocessor. The CU monitors the status of each of the sensors and devices and transmits this information to a Monitor Console. In addition to the sensors, stimulus devices are available that can be commanded by the CU to test each sensor. The test results are transmitted to the monitor console which displays to the operator the operational integrity of the remote area. All data transmissions between the CU and the monitor console are authenticated. The data transmission technique along with a data redundancy protocol is utilized to authenticate all communications. Also an audio surveillance channel, combined with a voice communications feature is provided between the CU (Remote area) and the monitor console.

The monitor console shown in Figure 3 provides the operator with several displays from which he can determine the status of the system or of an individual remote area. The monitor console displays include a geographic map display, a status information display, a graphics display, video displays (optional), and a printer to provide hard copy printout of all activities related to the system operation.

The FIDS can be configured for a wide variety of applications by selecting the appropriate equipment from the following list:

a. Monitor Console
b. Control Unit (CU)
c. Sensors

1. Ultrasonic Motion Sensor (UMS) with stimulus

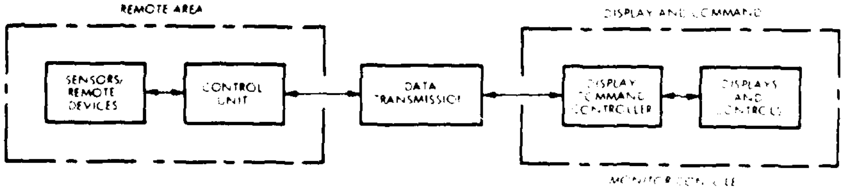


Figure 2. FIDS Simplified Block Diagram

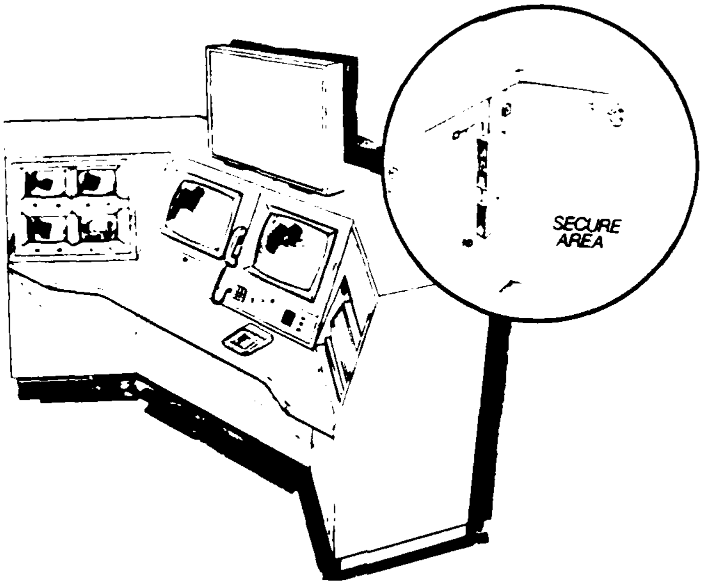


Figure 3. FIDS Monitor Console

2. Passive Ultrasonic Sensor (PUS) with stimulus
3. Capacitance Proximity Sensor (CPS) with stimulus
4. Balance Magnetic Switch (BMS) with stimulus
5. Vibration Sensor (VS) with stimulus
6. Passive Infrared Motion Sensor (PIMS) with stimulus
7. Duress Sensor

d. Audio Surveillance
e. Video Surveillance
f. Deterrents
g. Low Profile Console
h. Expanded Zone Monitor Console Option
i. Redundant Monitor Console Option
j. CU with redundant modem output
k. Satellite Control Processor (SCP) for expanded zones
l. Remote Status Monitor (RSM)
m. CMSD/MDTS Processor (CMP) for BISS interface
n. Associated CU and Monitor Console Power Supply
o. Sensor Communicator Interface for JSIIDS Sensors or Commercial Sensors
p. JSIIDS Control Processor for existing JSIIDS interface
q. Entry Control Device.

FIDS Monitor Console

General Description

The monitor console shown in block diagram form in Figure 4 functions as the command and control center for the system. Alarm and status information from the remote secure areas are displayed to an operator, stationed at the console, by means of two color CRT's, a printer and a geographic map display. An audio surveillance capability is available to provide additional information concerning an intrusion alarm in the form of audio signals from the remote area reporting the alarm. There are provisions in the console to include closed circuit television CCTV monitors for video surveillance of a protected area. An audio signalling device is provided to alert the operator of all alarm and status changes that occur in the operation of the system. To affort the operator with a capability to respond to the alarm and status changes a command keyboard is provided along with a voice communication panel including a telephone, capability to activate a radio communication link and/or establish voice communication with the remote secure areas.

Status Display. The primary display within the monitor console is the status information display. The status information for the total system will be presented to the operator in any alpha-numeric format with the use of color to hi-lite critical data. A sample display status is shown in Figure 5. The Control Unit status displayed as a minimum is as follows:

a. Control Unit identifier
b. Mode of CU operation
c. Standby power status
d. Alarm type
e. Commands actuated
f. Control Unit type
g. Control Unit priority
h. Request for voice communication with remote area.

The monitor console status data displayed is:

a. Standby power status
b. Tamper alarm conditions
c. Power supply component failures

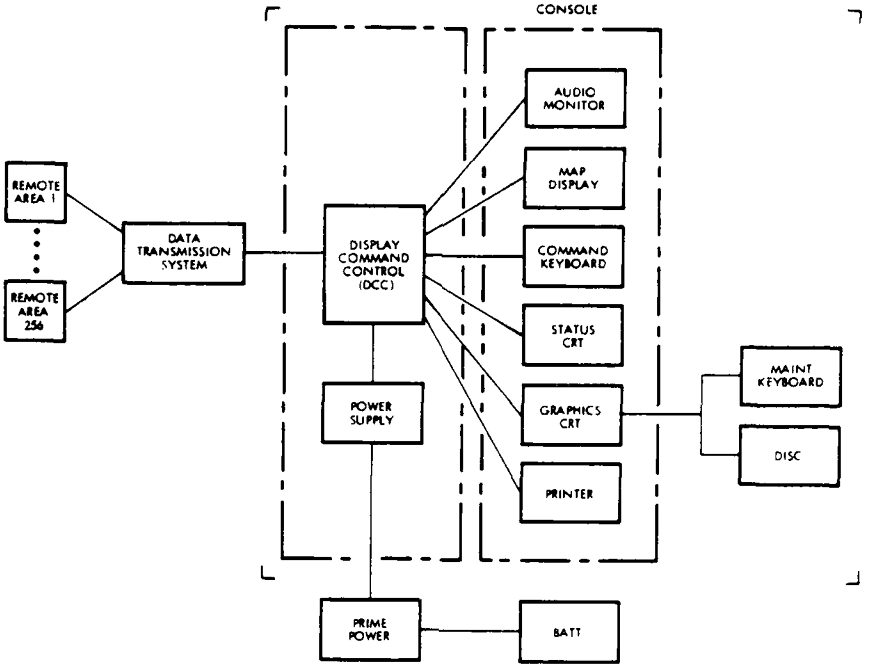
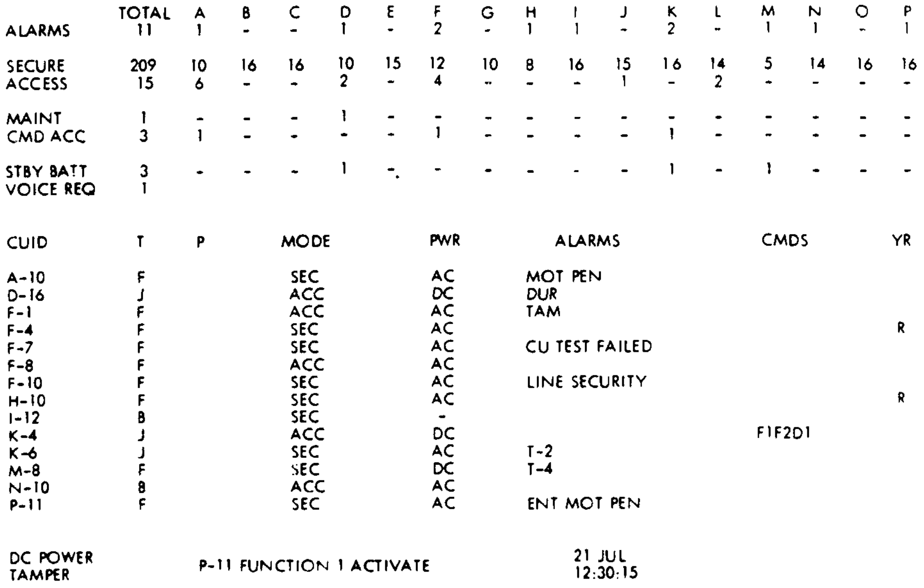


Figure 4. FIDS Monitor Console Block Diagram



```
           TOTAL  A   B   C   D   E   F   G   H   I   J   K   L   M   N   O   P
ALARMS      11    1   -   -   1   -   2   -   1   1   -   2   -   1   1   -   1

SECURE      209   10  16  16  10  15  12  10  8   16  15  16  14  5   14  16  16
ACCESS      15    6   -   -   2   -   4   -   -   -   1   -   2   -   -   -   -

MAINT       1     -   -   -   1   -   -   -   -   -   -   -   -   -   -   -   -
CMD ACC     3     1   -   -   -   -   1   -   -   -   -   1   -   -   -   -   -

STBY BATT   3     -   -   -   1   -   -   -   -   -   -   1   -   1   -   -   -
VOICE REQ   1

CUID        T     P      MODE      PWR      ALARMS             CMDS      YR

A-10        F            SEC       AC      MOT PEN
D-16        J            ACC       DC      DUR
F-1         F            ACC       AC      TAM
F-4         F            SEC       AC                                     R
F-7         F            SEC       AC      CU TEST FAILED
F-8         F            ACC       AC
F-10        F            SEC       AC      LINE SECURITY
H-10        F            SEC       AC                                     R
I-12        B            SEC       -
K-4         J            ACC       DC                         F1F2D1
K-6         J            SEC       AC      T-2
M-8         F            SEC       DC      T-4
N-10        8            ACC       AC
P-11        F            SEC       AC      ENT MOT PEN

DC POWER                                     21 JUL
TAMPER          P-11 FUNCTION 1 ACTIVATE     12:30:15
```

Figure 5. Sample Status Display Format

d. DCC failures
e. Processor or inter-processor communications.

Graphic Display. A second color CRT display, referred to as the graphics display, presents the physical configuration of a selected remote area. A sample graphics display is shown in Figure 6.

The graphic display provides specific information concerning the remote area physical configuration, installation of sensors, storage contents, and instructions to be followed by the operator in the event of alarms or abnormal status changes originating from the remote area. The graphic display can function as the status display in the absence or failure of the primary status display.

Command Keyboard. The command keyboard provides the means by which the operator can enter all system operational commands. The keyboard enables the operator to select a specific Control Unit for display of detailed status information and to selectively transmit commands to individual Control Units.

Map Display. The map display is a visual status board to which a geographic map is attached and on which locations and alarm conditions of the remote areas can be displayed. The remote areas displayed can correspond to the location of one or more FIDS control units or one or more individual BISS or REMBASS sensors.

The geographic map display provides the operator with an immediate overview of all remote areas and their respective alarm status in the form of lighted indicators placed in relative position of the remote area on a map of the base or facility. An alarm condition would be identified by an indicator being illuminated at the time an alarm occurs and would be extinguished when the operator resets the alarm condition via the command keyboard. (NOTE: alarm conditions can only be reset when the alarm status no longer exists.)

Audio Monitor. The audio montior within the console provides the operator with the capability to monitor audio from remote areas for which surveillance has been activated. Also 2-way voice communications can be conducted via the audio channel with personnel at remote areas. The audio monitor contains a louc speaker for monitoring of surveillance signals and a handset for operator communications via radio or a telephone system.

Printer. A printer provides a permanent record of alarm and tamper conditions and status changes of the secure areas, the montior console, and the data transmission system. All test results are printed with any failures identified and all operator command key actions are printed. The time of the occurrence of these events is also printed. All of the printed data is stored on disk for future recall.

Display and Command Controller.

The monitor consoles primary processing electronics are contained in the Display and Command Controller (DCC) as shown in Figure 7. The DCC contains all of the communications control interface to the remote areas, and provides the display control processing for each of the display devices. The DCC is configured with multi-microprocessors of the 8085 type.

The DCC is comprised of four main functional areas consisting of : modems, Line Control Processors (LCP's). CMSD interfaces, and two Display Control Processors (DCP's). There are 16 LCPs with an associated, dedicated modem. Each LCP/MODEM interfaces with up to 16 remote area Control Units. A spare (17th) LCP/MODEM is provided in the DCC as a back-up and can be switched in place of any of the other LCP/MODEMS.

Display Control Processor (DCP). The DCP is the main processor that makes up the network of processors contained in the Monitor Control. Its

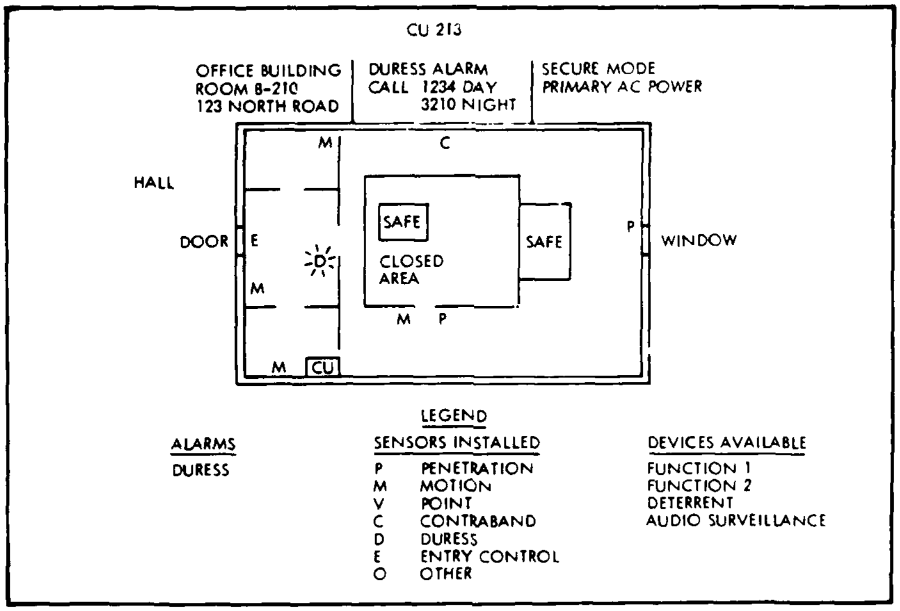


Figure 6. Sample Graphics Display Format

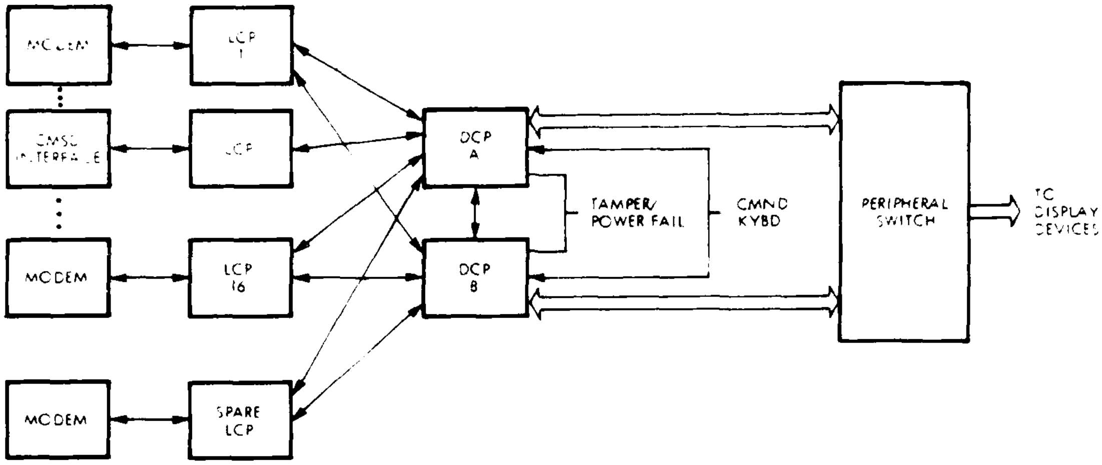


Figure 7. Display and Command Controller Block Diagram

function is to process data obtained from the line control processors, and output data to the displays to be presented to the operator. It also processes operator inputs, relaying them to the line control processors as commands, when appropriate.

As the central processor in the system, the DCP's role is crucial; therefore, its hardware and software is redundant in the form of dual processors, either of which can handle all of the processing, should it become necessary to take the other one out of operation.

Redundant circuitry is designed so that any component failure will not reduce the system below a minimally acceptable operational level. The approach is a modularized (or partitioned) communication and control system and status display system such that a single failure affects only a portion of normal system operation.

The peripherals are divided between the DCPs such that a minimal operational level is continuously maintained in the event of a single DCP failure. This modularized configuration and related status reporting provides the operator or maintenance personnel information about a failure and allows maintenance personnel to reconfigure peripheral assignments and display assignments during system operation. It is possible for either DCP to control any or all of the display system components.

The Command Keyboard is connected so as to communicate with both the DCPs. It is used by the operator to issue commands via the LCP's to the remote areas, and to modify information being displayed. The DCP checks keyboard commands for validity before transmitting them to the LCP for action.

Both DCPs are simultaneously interfaced to the command keyboard so that a failure of either DCP will not result in the inability to:

a. initiate any command
b. control the status graphic display
c. acknowledge any alarm or status change
d. reset any alarm conditions.

Line Control Processor. The line control processor (LCP) is a single circuit card assembly incorporating a 8085 microprocessor, memory, and associate control circuitry having the capability to function as a microcomputer. Its primary purpose is to communicate in an interrogate-respond mode via the modems with up to 16 remote area control units, pre-process the incoming data, check the validity of the data and then pass it on to both DCP's. The LCP also receives commands from the DCP's which are transmitted on to the remote area control units. The LCP continuously monitors the data link and reports any identifiable abnormality to the DCP. The LCPs have separate communication links to the two DCPs, and can thus be placed under the control of either one, or both, by software.

Hardware and/or software tests are continuously conducted such that each LCP is tested for proper operation when no higher priority tasks are awaiting execution. These tests consist of memory tests, and test of communications between LCP and DCP. Failure of any test and information relative to the failure is reported to the operator on the status display and recorded by the printer.

Sixteen LCPs and modems in the DCC are provided with a single LCP/modem backup to be utilized in the event of a failure in any single LCP or modem. Any LCP/modem failure is reported to the operator. This backup capability is under direct control of the operator or system maintenance personnel. The backup capability functions in the following manner. In the event of a failure in any LCP or modem, it is possible to assign the Control Units associated with the failed LCP and modem to the standby LCP and modem and for the console to resume full operation with communication to all Control Units without requiring that the operator gain access to the interior of the console electronic assembly.

Monitor Console Power Supply.

The Monitor Console Power Source supplies ac and dc power to the monitor console and incorporates a 24 volt lead acid rechargeable battery as an uninterruptable backup power source for up to 12 hours of operation in the event of any ac power failure. The power supply will operate from 95 to 125 VAC, single phase, 48 to 62 Hz. Also, in the absence of 95 to 125 VAC, will operate from 190 to 250 VAC, single phase, 48 to 62 Hz.

The Monitor Area Power Supply is partitioned with sufficient component redundancy such that a failure in any transformer, converter, regulator, or other subassembly will not cause loss of the total monitor system.

Control Unit

General Description

The Control Unit (CU) shown in block diagram in Figure 8 provides the interface between the Sensor, sensor stimuli, commandable devices, entry control systems, and the monitor console. Up to 48 sensors can be interfaced to a single control unit. The control unit monitors the status and alarm condition of the attached devices and formats all data responses for transmission to the Monitor Console. A microprocessor (8085 type) is used to implement the processing and control functions of the CU. The Control Unit performs the following functions:

a. Monitor the status of:

   1. Sensor intrusion alarms
   2. Entry Control Device entry approved/disapproved signal
   3. Tamper conditions
   4. Line Supervision alarms
   5. AC power failure status

b. Provide control and processing for:

   1. Interpreting and executing commands from the Monitor Console
   2. Inhibiting alarms during access mode
   3. Combined sensor alarm processing
   4. Sensor test
   5. Control unit self test
   6. Control (activation/deactivation) of external devices

c. Transmit information when addressed and interrogated by the monitor console.

CU operational capability. The control unit monitors one intrusion and one tamper alarm output from each of up to 48 sensors interfaced to the control unit. Each of the sensors will report its unique address and a type designation with each alarm/status report.

Information identifying control unit type (JSIIDS/FIDS), sensor types installed, stimuli installed, functions installed, deterrents installed, surveillance installed, voice communication configuration, and status of auto-arm processing is transmitted to the console.

In addition to all other alarm processing the control unit can be programmed to reject alarms from selected sensors. The system incorporates provisions to optionally select one or more sensor alarm types and an evaluation time period for each control unit. The alarm type(s) and time period(s) do not necessarily have to be the same for each control unit. Any alarm from a sensor of one of the selected types is not reported unless an alarm from a sensor of each of the selected types is received within the evaluation time period. This processing does not affect tamper alarm or self-test alarm processing.

Control Unit Testing. Any of the Control Units in the system can be tested whenever: (a) the Control Unit test command or system test command is initiated by the operator or maintenance personnel (b) the automatic system test sequence is initiated by the DCC in the monitor console. The automatic system tests are conducted at pseudorandom times during the course of any 24 hour period. If an intrusion alarm occurs at a Control Unit during a test, the testing is immediately terminated at the Control Unit and the alarm reported to the operator. A control unit test results in each of the connected sensor types being sequentially stimulated by the generation of sensor stimulus activating signals.

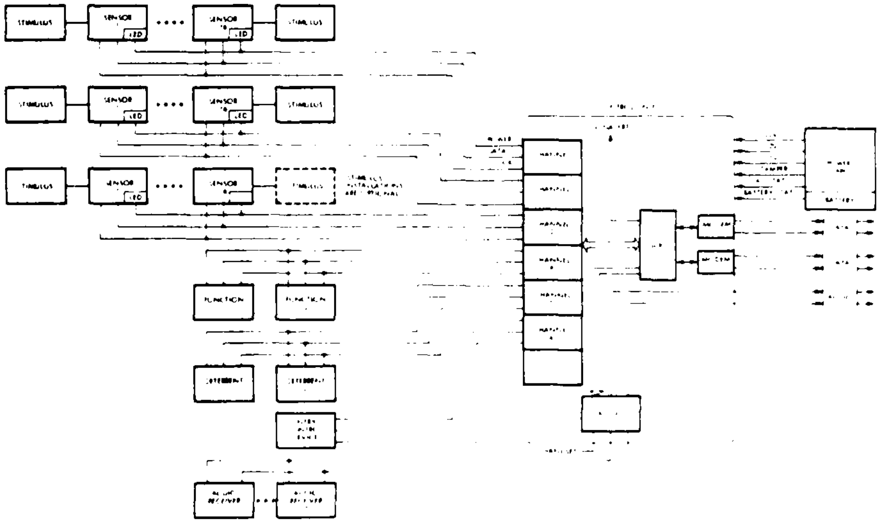


Figure 8. Control Unit Block Diagram

Commandable devices. Command recognized by the control unit include an audio surveillance command, four different commands to activate ancillary commandable devices and a voice communications command.

Secure Area Power Supply

The Secure Area Power Supply provides dc power for the Control Unit, sensors, function and deterrent devices, surveillance devices, entry control devices, and sensor stimuli in the secure area. The Secure Area Power Supply contains battery backup for up to 12 hours of operation following failure of the prime AC power. The supply will automatically switch to the standby (battery) supply upon loss of primary ac power. Standby power is provided by a 12 volt, lead acid, sealed (gelled electrolyte) rechargeable battery.

The power supply operates from 95 to 125 Vac, single phase, 48 to 62 Hz. Also, in the absence of 95 to 125 Vac, it can operate from 190 to 250 Vac, single phase, 48 to 62 Hz.

Data Transmission System

The Multipoint Data Transmission System (MDTS) provides a secure communications system between the monitor console and the control units. The data transmission protocol operates in an interrogate-response system to report alarm and status conditions at control units to a monitor console. The system will operate in a half duplex mode over a hard-wire link of up to 10 miles of proprietary No. 22 AWG twisted pair having noise characteristics no worse than a 3002 unconditioned channel. The data rate is 1200 bits per second and operation is asynchronous.

A method of authenticating the transmitted data is used to provide data security. The communication technique utilizes the capability of the microprocessors in the Line Control Processor (LCP) and the Control Unit (CU) to perform the processing necessary for data authentication and the implementation of the data transmission protocols.

The hardware provided for data authentication is a single integrated circuit which implements the Data Standard chosen by the National Bureau of Standards as a federal information processing standard (FIPS 46). The integrated circuit is a Western Digital DE-2001 which is compatible with the 8085 microprocessor used in FIDS. In addition to the hardware a software algorithm is implemented along with a protocol to increase the security of the data.

Sensor Communication

In other physical security system such as BISS and J-SIIDS as well as in commercial security systems, alarm reporting from sensing devices and control of remote devices has been accomplished primarily by relay contact closures. Typically many such sensors have been paralleled on a single alarm reporting line thus obscuring the identity of the alarming sensor. Furthermore, verification of line integrity has been performed by maintaining complex impedances across the alarm lines. Signaling to and from sensors has been limited to an intrusion alarm and a tamper alarm signal.

FIDS uses a sensor communication device in the form of a Large Scale Integrated (LSI) circuit for more comprehensive sensor communications. This technique provides:

a. Addressability to an individual sensor or remote device.
b. Sufficient generality for use with a variety of sensors, function devices, deterrents, entry control and surveillance devices.
c. Reporting to the control unit sensor configuration information, such as, sensor type and presence of a sensor stimulus.
d. Maintenance of line security via an interrogate/response system.
e. Provision for control of sensor stimulus as well as other functions.
f. Provision for reporting of status conditions in addition to intrusion and tamper alarms.

FIDS implements a Universal Asynchronous Receiver/Transmitter (UART) technique primarily for its flexibility and commonality with many standard data communications systems. This communications technique could be implemented with off-the-shelf components including an MSI UART plus several other SSI and MSI devices but would consume valuable circuit board space on each sensor device in which it is used. Thus, a custom LSI development to incorporate all of the required functions in a single circuit was developed for use with the FIDS sensor and can be used in a variety of other types of sensors.

The communicator circuit can interface with sensors having alarm relay contacts or a wide variety of solid state output drivers which are often used in lieu of relays. The communicator circuits can be installed in commercial off-the-shelf sensors by appropriate connection of flying leads provided with the communicator circuit module.

Conclusion

The FIDS is a system which, although having similarities to commercially available physical security systems, can not be matched by commercial systems in the following areas:

a. Human Factors Design of Monitor Console
b. High Security Data Authentication
c. Built-In Test Equipment
d. On-Line Maintenance Capability
e. Sensor Self-Test Features
f. Flexibility for Interfaces With Other Equipment
g. High Reliability Design (Provided by High Reliability Parts and Redundant Components)
h. Resistance to Compromise by Operating Personnel.

These features are required to provide a system which can meet the increasing sophistication of the threat while being capable of reliable operation and ease of maintenance.

JOB PERFORMANCE AND BRAIN ASYMMETRY: RELEVANCE FOR PHYSICAL SECURITY PERSONNEL*

G. W. Lewis, Ph.D.
Command and Control Systems
Navy Personnel Research and Development Center
San Diego, California 92152

ABSTRACT

Conventional paper-and-pencil personnel testing is able to predict academic performance fairly well, but not on-job performance. This may be due to heavy reliance on left hemisphere brain processing (verbal, analytical). On-job performance may place heavy demands on right hemisphere brain processing (spatial, simultaneous). Three research projects are described, which relate on-job performance to brain asymmetry as measured by visual event related brain potential (VERP) procedures. The three projects relate VERP measures to aviator performance in F-4 fighter aircraft, antisubmarine warfare trainee performance on a sonar simulator, and enlistee promotions over three years. One of our most consistent findings relates the VERP asymmetry standard deviation (SD) measure to performance for the personnel tested in these three projects. The asymmetry SDs are least for high performers and greatest for low performers in both front and back brain areas. Relevance in applying brain wave measures to physical security personnel areas is discussed. Future directions of behavioral research using noncontact (magnetic) recordings from the brain are suggested for physical security personnel assessment. Plans for investigating possible holography applications are also noted.

INTRODUCTION

This paper discusses the uses of brain wave measurement in predicting job performance. Three recently completed research projects in this area are described and future directions in physical security applications are suggested.

Paper-and-pencil aptitude tests contribute valuable information to employers, but they have been criticized for their ineffectiveness in predicting actual on-job performance. New kinds of tests are needed which will provide more complete understanding of the unique capabilities of each individual. Research on brain functions in the last several years suggests that certain brain wave tests may be able to predict nonacademic performance better than the conventional paper-and-pencil tests.

The brain has two hemispheres and has been shown to have at least two different modes of information processing. Verbal and analytic processing has been associated with left-hemisphere (LH) activity in most right-handed individuals. Part of the failure of the conventional tests to predict on-job performance is in their heavy reliance on left hemisphere functions. Spatial, simultaneous, and integrative processing has been attributed to right hemisphere (RH) activity. These two types of cognitive processing were initially discovered by anatomical studies using war wound, brain lesion, and "split-brain" subjects.

*The views expressed in this paper are those of the author and not necessarily those of the Department of the Navy.

More recently, these processes have been confirmed by modern computer technology and measures of brain electrical activity such as electroencephalographic (EEG) and event related brain potential (ERP) records (Bogen, 1969; Galin & Ornstein, 1972; Dimond & Beaumont, 1974; Callaway, 1975; Galin & Ellis, 1975; Knights & Bakker, 1976; Ornstein, 1977; Kinsbourne, 1978). EEG and ERP records show brain activity as extremely small electrical signals recorded from the scalp (few millionths of a volt). The EEG shows ongoing brain activity. ERPs are produced by sensory stimulation (e.g., light flashes). They are ordinarily obscured by large amplitude ongoing EEG activity. Advances in electronics and computer design have made possible the recording and measurement of ERPs. The use of the computer to record and average the ERP so that it may be seen against the background noise of the EEG has provided great momentum to research in this field.

The Navy Personnel Research and Development Center (NPRDC) established a research project in 1975 to investigate the possibility of using brain wave measures and other high-technology methods in personnel attributes assessment, classification, training, and performance prediction.

Two of our earliest research investigations related our visual ERP (VERP) measures to academic performance. The first (Lewis, Rimland, & Callaway, 1976) showed VERPs to be useful in predicting graduation among Navy remedial reading trainees. The second (Lewis, Rimland, & Callaway, 1977) demonstrated relationships between VERP measures and certain paper-and-pencil aptitude tests.

I would like to briefly describe three of our more recent investigations relating Navy on-job performance to brain activity. These include aviator performance in F-4 fighter aircraft, antisubmarine warfare (ASW) trainee performance on a sonar simulator, and number of achieved promotions by enlistees during the first three years of service.

Each of the three research investigations used the same hardware, software, and brain activity measures. The data were acquired either in our off-site laboratory at the Naval Training Center, San Diego or in a mobile laboratory at the Naval Air Station, Miramar, San Diego.

PROCEDURES

Eight channels of VERP data were acquired from four homologous sites on the left and right hemispheres as shown in Figure 1. These sites included frontal (F3, F4); central (C3, C4); parietal (P3, P4); and occipital (O1, O2). Each channel was referenced to the vertex (Cz). Subject ground was on the midline in the parietal region (Pz).

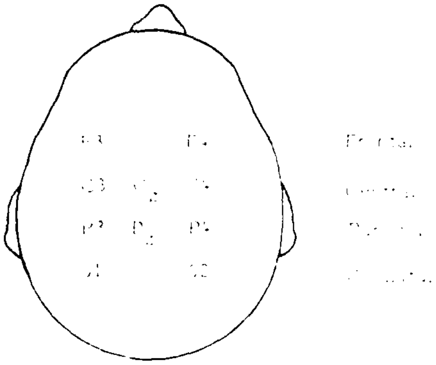


Figure 1. Electrode site montage.

The amplitude of each signal was determined in microvolt root mean square (μVrms) to provide a single number associated with each waveform. Figure 2 shows typical amplitude data at sites corresponding to the locations in Figure 1. The upper number at each site represents the μVrms value for the first 50 flashes, while the lower number represents the second 50 flashes. The waveforms for each 50-flash series are superimposed on the same baseline. For our purposes in this paper, the first and second flash series were averaged.

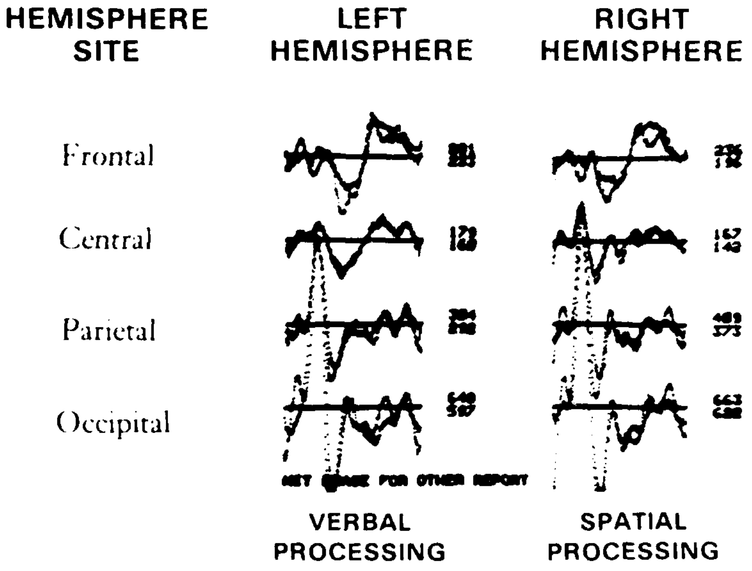


Figure 2. Sample VERP data amplitudes (μVrms).

VERP asymmetry is an index of the differences between the voltages produced at homolugous sites on the scalp. The asymmetry value equals the RH amplitude minus the LH (RH - LH). Four asymmetry values were obtained simultaneously at the frontal, central, parietal, and occipital sites for both hemispheres.

We have been very interested in not only right versus left differences as they relate to performance, but also front to back relationships. The asymmetry values for the frontal and central sites were averaged to provide the front measure, while the parietal and occipital asymmetry values were averaged to provide the back. Several interesting relationships have been observed in our laboratory regarding front versus back VERP asymmetry relationships and performance. Descriptive statistics [means and standard deviations (SDs)] were computed for each performance group. One of our most consistent findings relates front and back VERP asymmetry SDs to performance for the personnel tested in the three projects. The SD is a measure of dispersion and is one way to assess individual differences in our personnel performance groups. These findings will be described later.

Data were obtained on a field-portable computer system (Figure 3). The central processing unit was a Data General NOVA 2/10 equipped with a dual drive floppy disk unit, a small solid-state keyboard, an oscilloscope monitor, a fluorescent tube for visually stimulating the subject, and an integral eight-channel EEG unit. Calibration of the EEG unit and measurement of electrode impedance were under computer control. Visual stimuli were supplied by a commercial fluorescent tube with a custom-built power supply controlled by

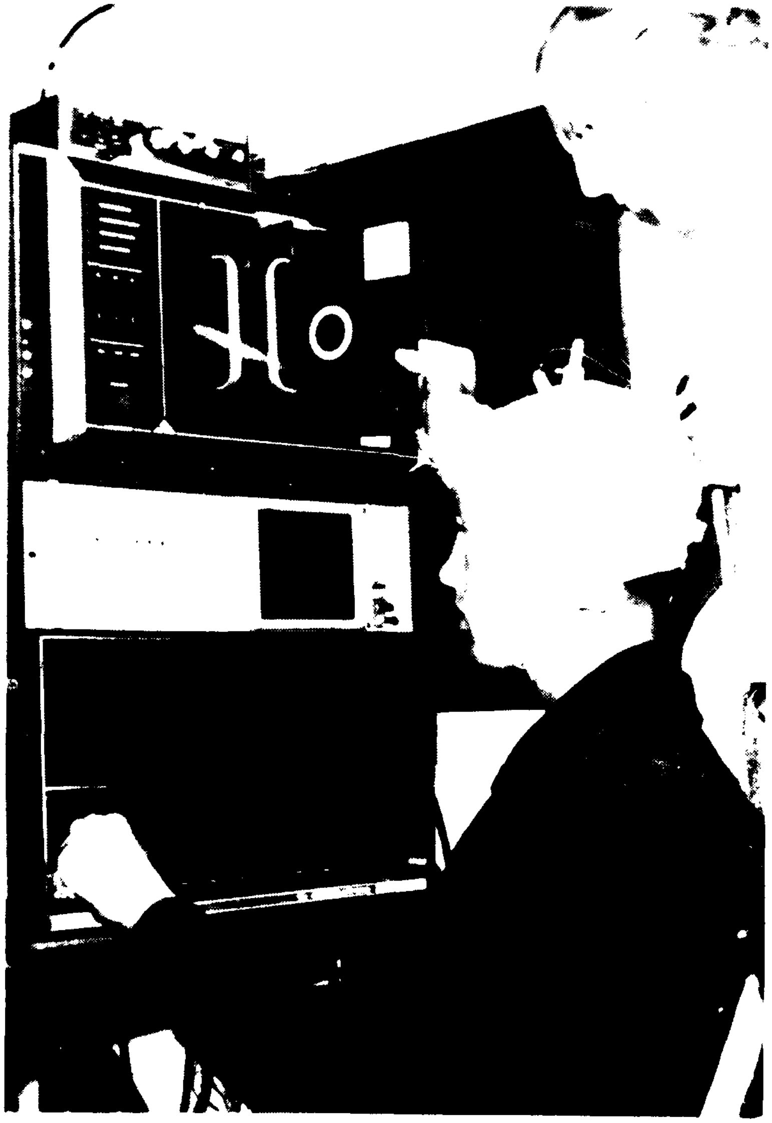


Figure 3. Subject wearing electrode helmet seated in front of computer system.

the computer. It illuminated a homogeneous white rectangle of approximately 7 x 15 inches (18 x 38 cm) placed one meter in front of the subject. Stimulus duration was 2 msec and luminance of the target approximately 3 foot-lamberts.

The subjects were prepared for recording after they had received brief instruction and had signed voluntary consent forms. After the technician had cleansed the hair and scalp at the electrode sites with an alcohol-impregnated cotton swab, a Lycra helmet was placed on the subject's head (see Figure 3). Lucite bushings, secured to the helmet, held the electrodes in place at the desired recording sites (Jasper, 1958). The electrodes were of the standard EEG recording type (Beckman miniature, 11 mm), each having a clear plastic extension tube attached and filled with electrolytic solution. A small sponge soaked with electrolyte held the solution in the tube and made contact with electrode paste on the scalp.

After all electrodes were in place and the impedance was checked (<5 KΩ), the subject was instructed to observe his real-time EEG activity on the oscilloscope display. He was then instructed to move his jaws, eyebrows, etc., so that he could observe how muscle artifact may contaminate the VERP data. The subject was then seated in a darkened room in alignment with the visual stimulus. A hand-held "time-out" switch was given to the subject which permitted him to suspend all stimulus presentation and analysis operations. He was instructed to press the switch to reject muscle artifact when he had to move, cough, etc.

RESULTS

Aviator Performance in F-4 Fighter Aircraft

The need to develop more effective methods of predicting on-job performance is one of the most severe challenges faced by personnel technology. It is estimated that training a single Navy pilot to combat readiness costs about $460,000 (North & Griffin, 1977). Attrition in naval pilot training from 1962 to 1977 averaged about 30% (Griffin & Mosko, 1977). Last year, in-flight accidents resulted in the loss of several aircraft, each costing millions of dollars.

In a recent review of the literature on aviator selection through 1977, North & Griffin (1977) pointed out that only 25-40% of the variance in aviator performance could be predicted, despite the use of an immense variety of previously available techniques. Although their 145-item bibliography represents an enormous investment in research effort and expense over a half-century period, the problem remains unsolved. There is clearly a need for improved methods of predicting the performance of naval aviators, as well as that of other personnel required to learn and perform highly demanding tasks.

During May 1976, we mounted our field-portable computer system in the NPRDC mobile laboratory facility to acquire VERP data from an F-4 fighter squadron of 58 aviators--28 pilots and 30 radar intercept officers (RIOs). We had three objectives in this research: first, determining the feasibility of recording data in an operational environment (these data are traditionally obtained in the laboratory); second, seeing if we could determine individual and group differences in our subject sample based on the VERP data; and third, relating performance of the aviators to our VERP amplitude and asymmetry measures (Lewis, 1979; Lewis & Rimland, 1979).

Figure 4 shows our laboratory van parked in the squadron hangar at the Naval Air Station, Miramar. Recording the very minute VERP signals in this operational environment proved feasible, even though there was a large amount of electrical and acoustical noise. We were able to quiet the electrical noise by using special optical coupling in the VERP amplifier and filter system, together with a special electrical transformer in the power line. Acoustical noise was reduced to an acceptable level by recording inside our van (designed with critical noise attenuating characteristics) and using white noise for masking.

Figure 4. Mobile VERP laboratory parked on-site in squadron hangar.

Pilots and RIOs might represent two different types of information processing served by the right and left hemispheres, respectively. Pilots must be able to respond to problems in three-dimensional space and make correct split-second judgments based on incomplete information (RH functions). Although RIOs must perform many pilot-like tasks, many of their duties require them to deal with information in a sequential and analytic way (LH functions). Obviously, pilots must also have good LH abilities, and RIOs good RH spatial abilities. Careful educational and psychometric screening of aviation candidates ensures that both pilots and RIOs have above-average intellectual abilities, particularly in the more readily measurable LH skills. However, the key elements of pilot and RIO performance might be categorized as primarily right- and left-hemispheric in nature, respectively. This suggests that the pilot group may be discriminated from the RIO group based on LH and RH VERP amplitude measures.

We found VERP differences between the pilot and RIO groups, accomplishing our second objective. These differences were greatest at C3 (left hemisphere central site, Figure 1; $F = 6.53$, $p < .02$) and F3 (left hemisphere frontal site, $F = 5.28$, $p < .05$). Because the selection criteria were very similar for both pilot and RIO groups, the differences between the groups may be due to training, experience, and job requirements. This brings us to our third objective, that of seeing if the VERP measures from these aviators may be related to their performance. As mentioned earlier, front and back asymmetry relationships with performance have been of great interest to us.

Each of the pilots and RIOs were placed into high- and low-performer groups based on flying proficiency as determined by the squadron Operations Officer. One way to assess both individual and group asymmetry differences at the same time is to examine asymmetry standard deviation (SD) values. One finding, which has been consistent in all three of the investigations being described in this paper, appears in Figure 5. This figure shows the SDs plotted for groups (pilots and RIOs), performance ratings (high and low), and electrode sites (front and back). Left-handed and ambidextrous subjects were removed because hemisphericity often tends to be mixed in these subjects. The SDs for both the high-rated pilots and high-rated RIOs were about equal at the front and back sites. Also, for both high-rated groups, the SDs were greater for the back than for the front sites. The SDs obtained for the low-rated groups at the front and back sites were much greater than those for the corresponding high-rated groups. Further, the SDs obtained for low-rated pilots at the front and back sites were greater than those obtained for low-rated RIOs at these sites. As with the high-rated pilot and RIO groups, the SDs for the low-rated pilot and RIO groups were greater for the back than for the front sites.

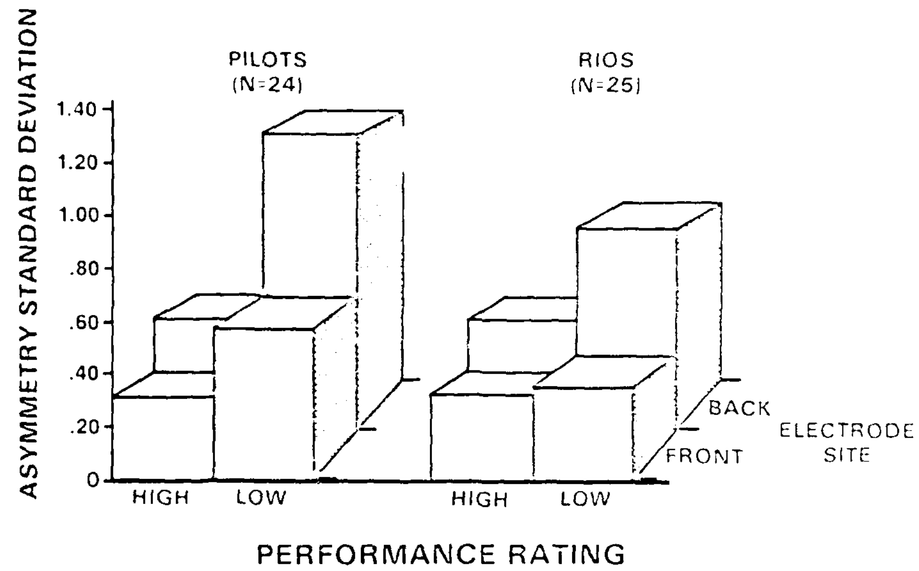


Figure 5. Asymmetry standard deviations for the high- and low-rated pilots and RIOs, front and back electrode sites.

The back electrode sites include a primary association area and the primary visual reception area. The front site includes both an association area and a sensory-motor area. The task required only observing a blinking light; no muscle activity was needed. The greater heterogeneity of the low-rated pilot and RIO groups as compared to the high-rated groups may be a result of the fact that there may be many ways to perform poorly, but few ways to perform well.

ASW Trainee Performance on a Sonar Simulator

The operator of today's sophisticated sonar equipment must perform difficult and demanding mental operations requiring quick processing of visual and auditory information and the visualization of moving objects in three-dimensional space. Although conventional paper-and-pencil aptitude tests are reasonably effective in predicting academic performance in sonar school, they are not effective in identifying those who are most likely to perform successfully as sonar operators.

One objective in this research effort was to determine if VERP measures could be used to improve the prediction of performance for sonar operators (Lewis, Rimland, & Callaway, 1978; Lewis & Rimland, 1980). We divided our sample of 26 ASW trainees into two groups (HIGH and LOW) based on their performance on a sonar simulator. The HIGH (N = 14) and LOW (N = 12) groups showed no differences in their paper-and-pencil aptitude test scores. However, substantial VERP amplitude (left hemisphere occipital site, F = 5.87, $p < .02$) differences were found.

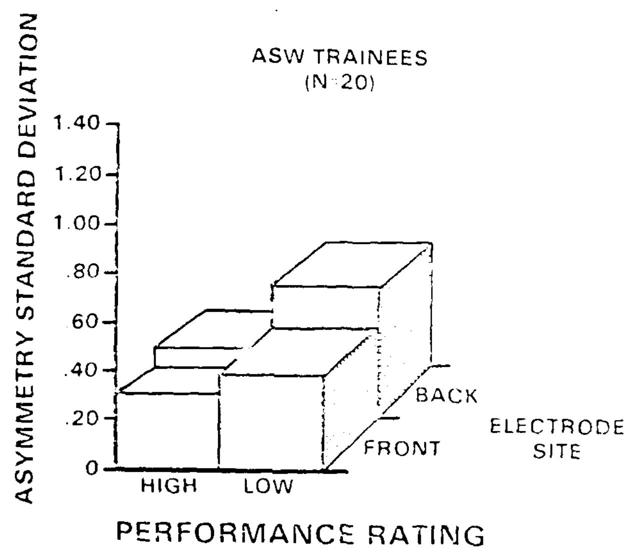


Figure 6. Asymmetry standard deviations for high- and low-rated ASW trainees, front and back electrode sites.

Relationships between asymmetry and performance for the ASW trainees were similar to those for aviators. These may be seen in Figure 6. Again we included only right-handed subjects (HIGH N = 10, LOW N = 10). The SDs, or dispersion of asymmetry measures, were very similar from the front to the back of the head for the H'GH group. Greater front to back differences were found for the LOW group compared to the HIGH group. Perhaps the HIGH performers were able to integrate and use their entire brain more effectively than the LOW performers. Finally, there was less dispersion in both front and back regions for the HIGHs compared with the LOWs.

Enlisted Promotion Rates

In a recently completed research project, we obtained follow-up performance records for enlisted recruits three years after recording the initial VERP data. Our objectives were to compare the VERP amplitude and asymmetry predictors with the traditional paper-and-pencil aptitude and academic predictors used by the Navy. We divided our sample (N = 252) into two groups based on the number of promotions each enlistee achieved during the preceding three years. The HIGH group (N = 134) had two or more promotions, while the LOW group (N = 118) had less than two promotions. VERP amplitude measures were able to differentiate the two groups and classify the subjects into either the HIGH or LOW group more effectively than did the traditional paper-and-pencil predictors.

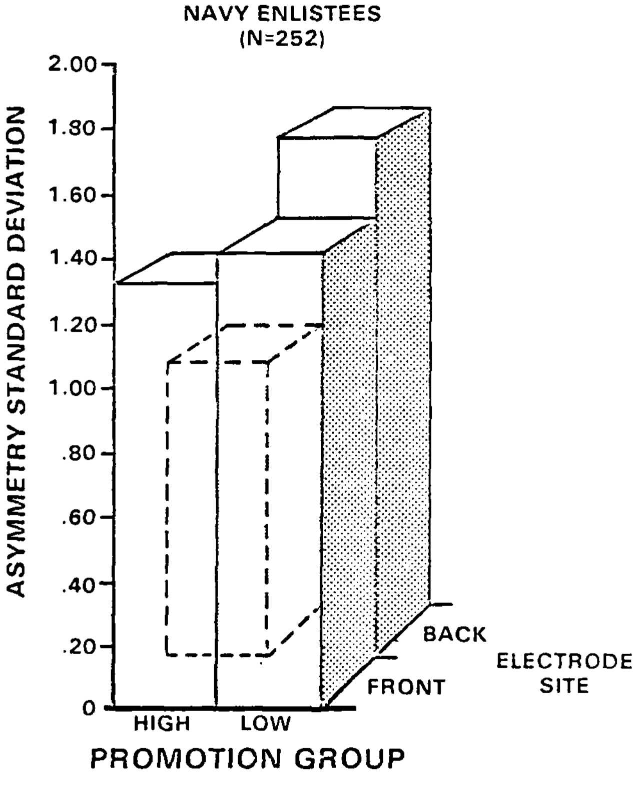


Figure 7. Asymmetry standard deviations for high and low erllistee promotion groups, front and back electrode sites.

Figure 7 shows similar asymmetry dispersion relationships for the enlistees as for the aviator and ASW trainee performance groups. Unlike the aviator and ASW trainee groups, left-handed and ambidextrous subjects were also included in

Figure 7. The front and back SD measures were less for the HIGH than for the LOW performance group. Also the front to back differences were greater for the LOW than for the HIGH group. One difference was observed for these subjects which was not observed for the aviator or ASW subjects. The HIGH group back electrode site SDs were less than the front for the enlistees, while it was slightly greater for the aviators and ASW trainees.

SUMMARY

One of the reasons we feel traditional paper-and-pencil aptitude tests predict academic performance fairly well, but not on-job performance, is that they tap the verbal, analytic processing performed by the left hemisphere. On-job performance requires much of the spatial, simultaneous processing performed by the right hemisphere. There have been many attempts to assess right hemisphere functioning by traditional testing procedures, but with little success. Procedures like the VERP may not only tap right hemisphere processing to a greater degree, but predict on-job performance more accurately than the traditional paper-and-pencil tests. Assessing individual differences with an emphasis on "process" rather than "content" variables as suggested by the concept of brain asymmetry may prove more successful in predicting human performance.

We feel we have made a start in applying new advances in technology and new information on brain functions toward predicting on-job performance. Several consistent findings have been observed in the various subject samples we have studied. One of the findings was reported here--relationships between asymmetry standard deviation measures and job performance. This suggests that VERP approaches may have widespread application to the general field of personnel assessment, training, and performance prediction. We have established an extensive library of brain wave predictor and performance follow-up data. These data have been acquired from both the laboratory and operational environments.

Our most recent work has been directed toward determining the feasibility of applying ERP technology to training. Initial results are promising and show that integration of the visual and auditory senses are critical to learning and training. Our objective in this work unit involves assessing the unique capabilities of each individual in order to increase training efficiency.

FUTURE DIRECTIONS IN PHYSICAL SECURITY APPLICATIONS

Our research over the last several years relating brain functioning to job performance may have direct relevance for physical security personnel. Much of the time spent by the physical security guard force is in an environment where often too little, rather than too much, activity occurs. In other words, these personnel are often requ'red to remain alert and vigilant (sustained attention) for long periods where little is happening. Jerison (1977) has suggested that vigilance may be assessed by the concept of brain asymmetry. He also suggests that selective attention and sustained attention may be very different behaviors and that the left hemisphere may be most involved with selective attention and the right hemisphere with sustained attention. Brain recording techniques similar to those described in this paper may be able to test Jerison's hypothesis and lead to better assessment of vigilance in physical security personnel.

Physical security personnel assessment, training, and performance predictions may be greatly enhanced by brain activity recordings. It may be feasible to establish consistent relationships between brain wave patterns and stable, dependable performance. Brain recordings may provide extremely important information in the area of personnel reliability, that is, assessing and predicting the performance of personnel under duress conditions (e.g., the family taken hostage by terrorists). It may be possible to determine a pattern of responses to a set of stimuli that can provide a basis for identifying personnel who are tolerant to stress conditions. Perhaps changes in the dependability of physical security personnel could be detected through periodic measurement of brain waves for comparison against earlier baseline records. This technique may be able to detect unusual stress problems, disgruntled crew members, or collusion by "insiders."

To date, our brain recordings have been obtained by using a traditional contact electrode procedure. We have been interested in a noncontact procedure for several years. Such a procedure may greatly speed data collection and may lower sensitivity to invasion of privacy restrictions. This new noncontact technology allows recording and measurement of magnetic activity from brain [magnetoencephalography (MEG)], muscle [magnetomyography (MMG)], and other body functions. Descriptions of this technology have been presented in several papers along with discussion of similarities (and differences) between the conventional contact recordings and the MEG/MMG noncontact recordings (Brenner, Williamson, & Kaufman, 1975; Cohen, 1968, 1972; Cohen & Givler, 1972; Reite, Zimmerman, Edrich, & Zimmerman, 1976; Sarwinski, 1977; Wikswo & Barach, 1980). We feel that with further development, the noncontact approach may prove very useful in assessing, training, and predicting performance of physical security personnel in the areas of vigilance and personnel reliability, for example.

Another area for future research directions of great potential benefit to physical security is holography. This technology allows the production of three-dimensional images from two-dimensional media, providing more realistic imaging of objects. The use of holography is already finding its way into education.

The Naval Surface Weapons Center, White Oak (NSWC/WO) is determining the feasibility of using holographic techniques to project false images for use in shipboard physical security systems. We expect to work with NSWC/WO in the behavioral aspects of holography (e.g., sensory deception of such false imaging techniques). Refractions for prescribing spectacle corrections are performed daily in eye clinics using the VERP technique. It would be possible to determine maximal quality of holographic images using our VERP procedures. Because holography assumes spatial processing (performed by the right hemisphere), it may be possible to assess sensory and cognitive factors associated with holography to determine individual differences in response to these images. Perceptual deception may be enhanced when we find out how the brain responds to holographic images. It may be possible to assign deception-resistant personnel to areas where false imaging techniques are used.

REFERENCES

Bogen, J. E. The other side of the brain I, II, III. *Bulletin of the Los Angeles Neurological Society*, 1969, *34*, 73-105, 135-162, 191-220.

Brenner, D., Williamson, S. F., & Kaufman, L. Visually evoked magnetic fields of the human brain. *Science*, 1975, *190*, 480-482.

Callaway, E. *Brain electrical potentials and individual psychological differences*. New York: Grune and Stratton, 1975.

Cohen, D. Magnetoencephalography: Evidence of magnetic fields produced by alpha-rhythm currents. *Science*, 1968, *161*, 784-786.

Cohen, D. Magnetoencephalography: Detection of the brain's electrical activity with a superconducting magnetometer. *Science*, 1972, *175*, 664-666.

Cohen, D. & Givler, E. Magnetomyography: Magnetic fields around the human body produced by skeletal muscles. *Applied Physics Letters*, 1972, *21*, 114-116.

Dimond, S. J. & Beaumont, J. G. (Eds.). *Hemisphere function in the human brain*. New York: John Wiley, 1974.

Galin, D. & Ellis, R. R. Asymmetry in evoked potentials as an index of lateralized cognitive processes: Relation to EEG alpha asymmetry. *Neuropsychologia*, 1975, *13*, 45-50.

Galin, D. & Ornstein, R. Lateral specialization of cognitive mode: An EEG study. *Psychophysiology*, 1972, *9*, 412-418.

Griffin, G. R. & Mosko, J. D. *Naval aviation attrition 1950-1976: Implications for the development of future research and evaluation* (NAMRL-1237). Pensacola: Naval Aerospace Medical Research Laboratory, August 1977.

Jasper, H. The ten-twenty electrode system of the International Federation. *Electroencephalography and Clinical Neurophysiology*, 1958, *10*, 371-375.

Jerison, H. J. Vigilance: Biology, psychology, theory and practice. In Mackie, R. R. (Ed.), *Vigilance: Theory, operational performance, and physiological correlates*. New York: Plenum Press, 1977, 27-40.

Kinsbourne, M. (Ed.). *Asymmetrical function of the brain*. New York: Cambridge University Press, 1978.

Knights, R. M. & Bakker, D. J. *The neuropsychology of learning disorders: Theoretical approaches*. Baltimore: University Park Press, 1976.

Lewis, G. W. Visual event related potentials of pilots and navigators. In Lehmann, D. & Callaway, E. *Human evoked potentials: Applications and problems*. New York: Plenum Press, 1979. (Proceedings of the NATO Conference on Human Evoked Potentials held at Konstanz, West Germany, 26-29 August 1978. Sponsored by the NATO Special Program Panel on Human Factors).

Lewis, G. W. & Rimland, B. Hemispheric asymmetry as related to pilot and radar intercept officer performance (NPRDC Technical Report 79-13). San Diego: Navy Personnel Research and Development Center, 1979. (AD-A068 087)

Lewis, G. W. & Rimland, B. Psychobiological measures as predictors of sonar operator performance (NPRDC Technical Report 80-26). San Diego: Navy Personnel Research and Development Center, May 1980.

Lewis, G. W., Rimland, B., & Callaway, E. Psychobiological predictors of success in a Navy remedial reading program (NPRDC Technical Report 77-13). San Diego: Navy Personnel Research and Development Center, December 1976. (AD-A037 339).

Lewis, G. W., Rimland, B., & Callaway, E. Psychobiological correlates of aptitude among Navy recruits (NPRDC Technical Note 77-7). San Diego: Navy Personnel Research and Development Center, February 1977.

Lewis, G. W., Rimland, B., & Callaway, E. Visual event related potentials: Toward predicting performance. In Callaway, E., Tueting, P., & Koslow, S. H. Event related brain potentials in man. New York: Academic Press, 1978. (Proceedings of the Event Related Brain Potentials in Man Conference, held at Airlie House, Virginia, 26-29 April 1977. Sponsored by the Clinical Research Branch, National Institute of Mental Health, Rockville, Maryland).

North, R. A. & Griffin, G. R. Aviator selection 1919-1977 (NAMRL Special Report 77-2). Pensacola: Naval Aerospace Medical Research Laboratory, 1977.

Ornstein, R. E. The psychology of consciousness (2nd Edition). New York: Harcourt Brace Jovanovich, Inc., 1977.

Reite, M., Zimmerman, J. E., Edrich, J., & Zimmerman, J. The human magnetoencephalogram: Some EEG and related correlations. Electroencephalography and Clinical Neurophysiology, 1976, 40, 59-66.

Sarwinski, R. E. Superconducting instruments. Cryogenics, December 1977, 671-679.

Wikswo, J. P., Jr. & Barach, J. A. Magnetic field of a nerve impulse: First measurements. Science, 1980, 208, 53-55.

INSTRUMENTATION FOR SECURITY FORCE EVALUATION AND TRAINING

M. A. Ondrik and C. E. Wold
The BDM Corporation, Albuquerque, New Mexico 87105

INTRODUCTION

During the past few years numerous organizations have developed mathematical models and computer codes which address the problems of security of strategic materials. These models address topics ranging from mechanical models of the equipment employed to psychological models of the personnel involved. However, realistic force-on-force free play field experiments are necessary to calibrate and evaluate these models if they are to be of predictive value in the future.

A new generation of instrumentation is now being developed under the Theater Nuclear Force Survivability, Security, and Safety Program (TNFS^3) sponsored by the Defense Nuclear Agency. This instrumentation will provide the realistic weapon simulation and data acquisition capabilities required to address these issues. Historically, the users of instrumentation have not had a clear perception of the kinds of data that could be acquired if they only asked for it; and the instrumentation designers have not had a clear understanding of the kinds of data that would be most useful in calibrating a model or verifying a theory. Designers have traditionally provided for acquisition of the kinds of data that seemed useful to them, e.g., player position, engagement parameters, etc. Analysts have traditionally requested the kinds of data that they thought the instrumentation could provide - typically in the form of requirements - hoping that these data could be sufficiently massaged to provide some insight into the behavior of the parameters in which they are truly interested.

It is the purpose of this paper to introduce to potential users a new generation of instrumentation designed to acquire and record virtually any information which can be measured electronically. It is our hope, as designers, that this paper will stimulate the readers, as potential users, to make available descriptions of the kinds of data that are really desired in the form of a dialogue rather than as a requirements document. Such dialogue can contribute to an instrumentation system which directly acquires the "correct" data (not always obvious) for the process at hand. This should result in a much more fruitful interaction between the test planners, analysts, and instrumentation specialists and provide for a much more efficient and cost effective approach to achieving our common goal.

THE INSTRUMENTATION SYSTEM

The TNFS³ instrumentation system, shown in figure 1, is built around three major subsystems which utilize to the greatest extent possible identical hardware modules.

Each player (human, vehicle, etc.) carries his own Player Pack. The Player Pack performs all the necessary data acquisition and processing for that particular player. Specific functions performed are: position location, real-time casualty assessment, event time tagging, weapon simulation and detection, communications with the central site, and data storage.

The central site performs the command and control features (start test, stop test, recall); handles indirect fire simulations; records and monitors real-time data if desired; and performs the operations, maintenance, and quick-look data reduction functions.

The final element is the RF communications subsystem. It provides the central site to players communications link via a network of RF repeaters. The RF repeaters can also configure themselves as individual RF transponders for use in determining player position location.

The instrumentation has been developed using a highly modular design approach and distributes the real-time processing to each individual, thereby reducing the real-time telemetry bandwidth requirement and the need for a large central computer complex.

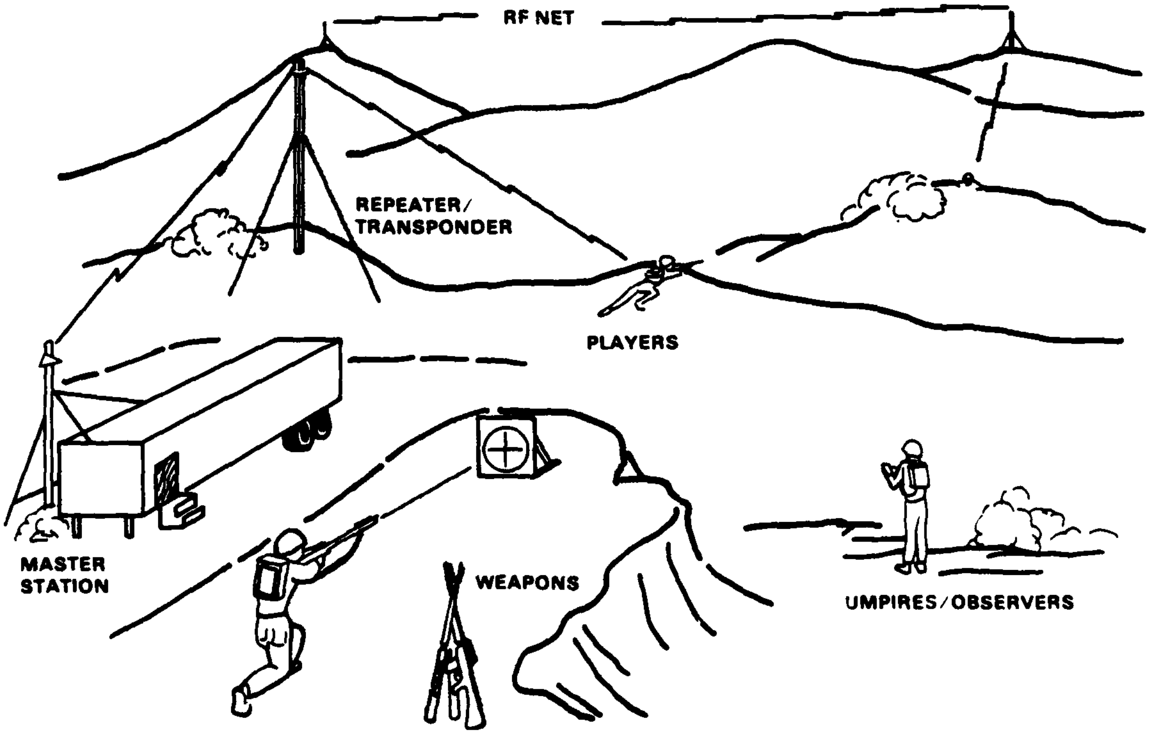


Figure 1. The Instrumentation System Elements

Technical implementation required the folding-in of the functional, operational, and economic characteristics of the system as a whole. Specific operational factors considered were:

(1) Modularity - The addition of players will not require system re-engineering or software reconfiguration.

(2) Mobility - The system can be easily moved and rapidly assembled at test sites in the U.S. and Europe.

(3) Graceful Degradation - The system does not fail in a catastrophic mode but by individual players.

(4) Adaptability - The system can be directly converted for training usage.

Heavy emphasis has been placed on human factor engineering and the impact of the player instrumentation on engagement realism. Some of the factors considered were:

(1) Player Mobility - The size, weight, and body attachment must not hinder an individual's mobility or cause him/her to react differently from under normal circumstances.

(2) Transparent to the Player - The player is not required to engage in any activity related to the operation of the instrumentation.

(3) Provide No Negative Training - The instrumentation must not provide the players with any data he would not normally have e.g., remaining ammo count or the need to fire blank ammo.

THE PLAYER PACK

The recent availability of powerful, single-circuit microprocessors and large-scale integrated circuits has made it possible to perform position location, data acquisition, processing, and recording with compact instrumentation carried by individual players. It is the Player Pack that forms the core of the force-on-force instrumentation. As shown in figure 2, it consists of a 10-pound unit carried in a soft pack and a 2-pound power unit contained in a conventional ammo pouch.

The primary element of the Player Pack is a microcomputer. This element provides the instrumentation with the flexibility needed to address the wide range of data acquisition requirements identified by the test planners. In addition to the microcomputer, there are additional hardware modules designed to perform specific functions such as weapon simulation, weapon engagement detection, position location, data storage, and communications for instrumentation control. All of these functions are performed in a transparent fashion; the player need not engage in any

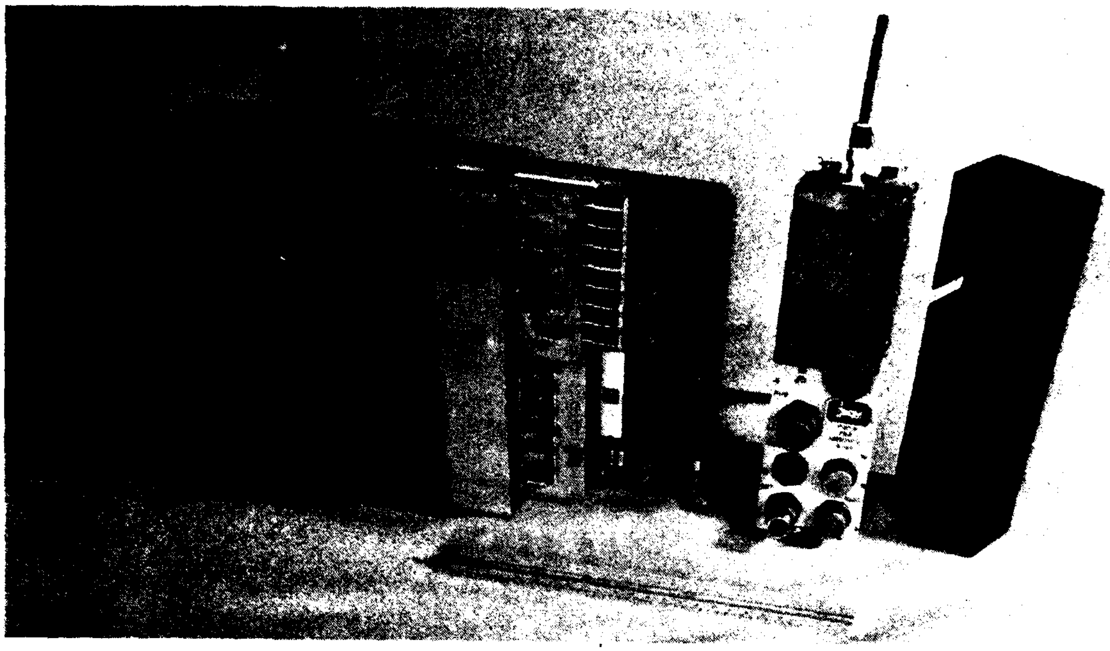


Figure 2. The Player Pack - Small, Lightweight, and Highly Modular

activity or operation that he would not normally perform if he were not instrumented. Specific modules are included in the Player Pack on as as-needed basis, dependent upon the player's function in the particular scenario.

The modular concept coupled with a standard interface allows future improvements in technology to be easily incorporated with no adverse impact on the remainder of the system.

An example of the Player Pack's data acquisition and processing capability is real-time casualty assessment (RTCA). Casualty assessment has long been the most difficult aspect of force-on-force testing in terms of realism. Umpires have traditionally been used for this purpose but, as in any game, there have always been many questionable results and subsequent invalid decisions. Currently, large amounts of raw data and large-scale computer systems are required to perform real-time casualty assessments for a limited number of participants at firing rates typical of mobile artillery.

For short-range engagements with human players (10-300 meters) the problem of accurate RTCA has become difficult. The targets are normally humans. Because weapon lethality is critically range dependent, the engagement distance between players must be known very accurately (3-5 meters). Furthermore, at these ranges, previously ignored engagement parameters begin to have a great influence on the outcome of the engagement. Variables such as firer posture, firer marksmanship, weapon type, ammunition type, target aspect, target body armor, hit point, and range must be included in the determination of the probability of kill algorithm.

To further complicate the issue, the casualty assessment must be completed within the normal "response time" of the engaging players to avoid the situation where a "dead" player "kills" another before he is notified that he is "dead."

Until recently, such real-time casualty assessments, including the aforementioned parameters, were not technically feasible. The player instrumentation shown in figures 3 and 4, provides this capability. Furthermore, because each Player Pack is concerned with only the individual player (distributed processing) the number of players can be increased, without limit, with no impact on the real-time response of this overall system.

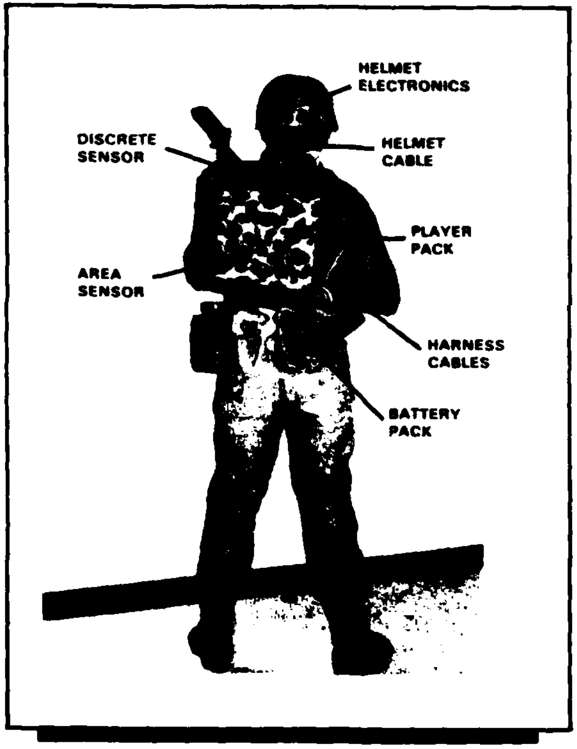


Figure 3. Player Instrumentation Rear View

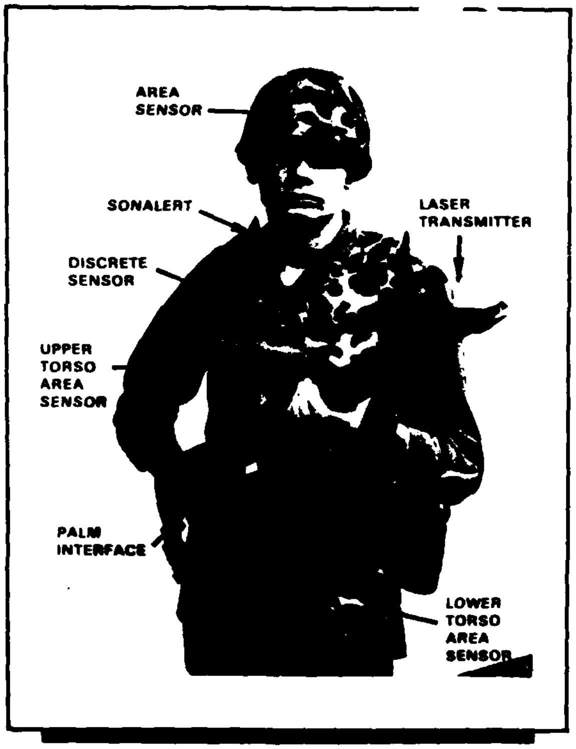


Figure 4. Player Instrumentation Front View

With this instrumentation, attack and security forces of any size may be paired against each other. Training effectiveness can be assessed by force-on-force scenarios played at various times under varying conditions during the training program. Furthermore, variables such as marksmanship and weapon type can be changed by the Master using the RF link, thus enabling rapid assessment of the probable impact of enhanced firearms, training, or different weapons in the effectiveness of the security forces.

IMPLICATIONS FOR BEHAVIORAL RESEARCH

The TNFS^3 instrumentation was designed primarily to resolve issues regarding physical security, remote sensing devices, security force response times, etc. However, it is a powerful data acquisition tool that can be used by the behavioral science community to collect human physiology data, under realistic environments and with the participants, and the resulting data, unaffected by heavy or nontransparent instrumentation.

The modular hardware and software structure allows the incorporation of new sensors and processing modules with no impact on the baseline instrumentation capability. Additions such as EEG, EKG, blood pressure, and body resistivity can and will be added as their requirements surface.

Security force personnel can be tested under controlled conditions and their performance level can be evaluated versus the following:

(1) Physical Condition

(2) Intelligence Quotient

(3) Degree of Training Received

(4) Fatigue

(5) Boredom

(6) External Environment

SUMMARY

The TNFS^3 instrumentation hardware and software elements have been designed with the element of change in mind. The distributed system is modular and mobile, degrades gracefully, requires little field support, and is easily adapted to respond to new requirements. The initial operational capability of March 1982 is still sufficiently distant for your specific requirements to be incorporated. EKG, EEG, body resistivity, etc., can be be included only if the requirements are identified early by the users.

REFERENCES

1. Draft - Final Report of Instrumentation for PARAFOX VII, U.S. Army Combat Development Experimentation Command.

2. Final Report - Early Development of TNFS^3 Test Capability, BDM/TAC-78-545-TR, 26 December 1978.

3. F156-77, Vega Model 6133 Multi-Vehicle Positioning System, Vega Precision Laboratories, Inc., Vienna, Virginia, 16 August 1977.

4. GUARD Phase I Report, BDM/TAC-78-30-TR, for the Sandia Laboratories, 30 June 1978.

5. Infantry Direct Fire Simulator System, Operation and Preventive Maintenance Manual, Revision A, International Laser Systems, Inc., for the U.S. Army Combat Developments Experimentation Commands, Fort Ord, California, January 1976.

6. Lawhead, N., "Position Location Systems Technology," IEEE Position Location and Navigation Symposium, November 1976, pp. 1-12.

7. Multiple Integrated Laser Engagement System, Xerox Electro-Optical Systems, Pasadena, California.

8. Position Location Reporting System, System Technical Description, Hughes Aircraft Company, General Systems Group, for the U.S. Army Electronic Command, 15 September 1977.

9. Real Time Casual Assessment Handbook, Vol. II., Casualty Assessment Parameters, 1 August 1977, BDM Services Company.

10. Theater Nuclear Force Survivability and Security Instrumentation, BDM/TAC-78-490-TR, 30 November 1978.

11. Theater Nuclear Force Survivability and Security Measures of Effectiveness, BDM/W-78-664-TR, 31 January 1979.

DISCUSSION

QUESTION FROM THE FLOOR: Do you have any way to record wounds, rather then just full kills?

MR. WOLD: Yes, we are capable of both wounds, kills and near-misses. When you receive a laser message, you can calculate a probability of hit.

However, you look at where your ranges from the target player were to the firing player. If a sufficient number of sensors were or were not eliminated, you can then do a simulation of a hit and wound situation.

Typically, if you are within 50 m with an M-16, you look at the lethality table. With that type of beam, you should have a beam of about 8 in. You should have at least one area sensor. You will know, basically, if he was shot in the upper chest, lower chest, or head. But, we can play and simulate near misses and wounds.

QUESTION FROM THE FLOOR: Do the players notify those wounded?

MR. WOLD: That is correct, and we can also play marksmanship level. Under those cases, we could actually decrease his marksmanship level during that period. Some of the tests show that there are periods when, with up to three body wounds, the player still operates, but in a somewhat degraded fashion.

QUESTION FROM THE FLOOR: Do you have any data to indicate the correlation with mal-ammunition? What is the difference between what you might expect using mal-ammunition and your laser?

MR. WOLD: Well, we are basically using the data available for this that has been validated at two bases. So, basically, the scenarios that typically identify it under probe data that we are developing it for are relatively short--inside of 300 m, usually. A physical security site is usually 200 m by 200 m. Therefore, the ballistics are really not that critical.

QUESTION FROM THE FLOOR: You are within 300 m.

MR. WOLD: Typically, yes.

QUESTION FROM THE FLOOR: Could you tell us something about the development and time frame for this system?

MR. WOLD: We are entering right now into the development phase utilizing three or four computer packs. In November we hope to have 10, and in May, with those 10 and approximately five repeater stations, enter into the system we are testing.

In July 1981, we hope to have a go ahead for production and the production units will be 50 player units, 15 repeater units, and the master station which we hope to have in the first quarter of fiscal year 1982.

GUIDAR Alarm Assessment

Dr. R. Keith Harman
James H. Chalmers
Computing Devices Company

Introduction

The basic guided radar concept presented in previous papers [references 1 and 2] is essentially a moving target indicator bistatic radar using "open-waveguides" as the two antennas. As illustrated in Figure 1, an rf signal is transmitted along one cable to be terminated in a matched load. Energy travelling outside the leaky coaxial cable couples into the adjacent receive cable. While some of the coupled energy continues in the codirection to be terminated in a matched load, the coupled energy of particular interest returns in the contradirection to the receiver. This received signal is then demodulated and processed to detect targets which affect the coupling between the cable transducers. A CW signal may be transmitted if only the presence of a target along the transducer is required. If target location is also required then a pulsed or pulse-coded modulation may be used to locate the target since the time delay from transmission of the pulse to reception of the target induced change is proportional to the distance the target is along the sensor length.

The design of the leaky cable transducer is a significant factor in determining the sensor performance. Figure 2 illustrates eight different leaky coaxial cable designs which have been tested. Clearly there are two basic parameters to be optimized in a cable design: the along line attenuation and the coupling factor. In a contradirectional sensor it is highly desirable to 'grade' the cable; in other words, increase the coupling along the sensor length to account for the cable attenuation. In a properly 'graded' cable the transmitted field strength and the receive susceptibility are uniform along the entire transducer length. As in normal coaxial cable design the attenuation per unit length decreases with cable diameter (constant frequency and impedance), with increasing conductivity of the inner and outer conductors and with a reduction in the dielectric constant of the insulating material. This dielectric constant is the dominant factor in determining the velocity of propagation; a vital factor in the sensor design. The coupling factor is a very complex function of the number of holes in the outer conductor, the exposed area and the aspect ratio of each hole. In general a cable with many small holes (d) is not as good as one with fewer but larger holes such as (a), (b) or (c). The cable attenuation increases with frequency much like normal coaxial cables; however, the coupling is relatively constant with frequency over the 30 to 90 MHz band.

Since the leaky cable transducer is in essence an 'open waveguide' or a 'surface waveguide' the medium surrounding the cable has a profound effect. If the medium is 'lossy' then the sensory sensitivity to targets will be reduced. In addition, the velocity of propagation in the medium surrounding the cable relative to that inside the cable can cause 'mode cancellations' or periodic 'dead-spots' along the sensor length under certain conditions. This 'open waveguide' concept has been very useful in developing a sensor model based on simple transmission line theory and the associated theory of continuously coupled parallel transmission lines. This model enables one to accurately predict sensor performance as a function of the medium surrounding the cables. Since this model has been developed under Company funding it is considered proprietary and hence will not be discussed in this paper. Nevertheless some of the results will be presented later to illustrate the profound effect the burial medium has on sensor performance.

In the basic sensor concept illustrated in Figure 1 there is a fixed return at the receiver without a target present. This return is called the 'profile' of the installation, a function determined by cable spacing, cable imperfections and burial medium. The ratio of target response to profile determines the dynamic range requirements of the sensor. The magnitude and stability of the profile has a major effect on the sensor false alarm rate.

It should be noted that one could design a sensor based on co-directional coupling; in other words, placing the receiver at the opposite end of the receive cable. This is attractive in that it does avoid the need for cable grading. It does, however, produce several very difficult problems:

1. there is no target location information in such a sensor, thereby forcing one to deploy it as a 'block' sensor,

2. the target to profile ratio is dramatically reduced which causes a dynamic range problem,

3. the profile is much more sensitive to environmental changes,

4. the processing cannot utilize the target phase information, and

5. the electromagnetic field strength and susceptibility to external signals varies along the sensor length.

In simplistic terms one can see that a target has the same phase response at any location in the sensor field since the cables essentially operate in a TEM mode and the signal path length is independent of target position. In a contra-directional system the target phase changes with distance along the sensor. If one considers the profile as the composite of many minute fixed targets, it is clear that the response adds up in the codirectional sensor and tends to cancel out in a contra-directional sensor. Based on our theoretical model and considerable number of field tests, it is concluded that the slight additional cost of cable grading is more more acceptable than the inherent poor performance of a co-directional leaky cable sensor.

The selection of operating frequency and bandwidth requirements for a contradirectional leaky cable sensor are very similar to radar design. One factor which must be considered is the target cross section. In the case of a human target and a buried cable sensor the response due to the human feet is much stronger than that from the head or arms. This is illustrated qualitatively in Figure 3. This cross section tends to be maximized in the 60 to 90 MHz frequencies. The bandwidth requirement for a pulsed system is basically related to the desired target resolution. (The minimum distance between two targets such that they are detected as two targets as opposed to one.) This calculation must take into account the velocity of propagation inside the cable transducer. (Typically 79% for foamed polyethylene and 88% for low density foamed polyethylene.) Note that about 10 Hertz bandwidth required for a CW sensor providing target detection without location. Location accuracy is largely a function of the signal to noise ratio; a factor which is directly dependent on transmit power.

The transmit power requirement is a function of the cable coupling (at the start of the graded cable), the attenuation in the burial medium, the receiver thermal noise level and the desired signal to noise ratio to achieve the desired false alarm rate and location accuracy. In a contradirectional sensor the transmitted field strength is uniform along the sensor length and should be constrained to meet FCC regulations governing low power radiation devices.

In addition to a pulsed GUIDAR sensor, Computing Devices also manufactures a continuous wave (cw) intrusion detection sensor called the Short Perimeter Intrusion Radar (SPIR). The SPIR sensor protects a perimeter of length 255 metres (830 feet) using a processor that operates out of doors, typically to protect individual aircraft. This sensor, being cw, does not divide the perimeter into range cells but indicates only the presence or absence of a target over the whole perimeter. Its detection output is taken to a panel which displays the output from several sensors.

The discrimination against small (nuisance) targets is achieved by the response of the sensor as a function of target mass. With a 180-pound human as a reference, the response of the sensor to a 75-pound human is only 5 decibels, whereas to a 20-pound animal it is 20 decibels down. As the animal mass decreases below 15 pounds, the response drops off very rapidly. Thus discrimination against small animals is achieved by setting the target threshold somewhere between the response to a 10-pound animal and a 75-pound human.

Display Panel of the Current GUIDAR Processor

The GUIDAR system has a display shown in Figure 4. The perimeter is divided into 32 display zones labelled A1 through A16 and B1 through B16. The presence of an intruder in a display zone is indicated by an audible alarm (horn) and a flashing light associated with that display zone. A perimeter of up to two miles can be monitored by one GUIDAR unit.

The perimeter is divided into range cells each 33.3 metres long. If the total perimeter does not exceed 1-1/3 miles, each display zone represents two adjacent range cells. When the perimeter exceeds this length, three range cells are associated with one display zone. So, although detection of intruders is done on range cells 33 metres long, the operator sees alarm indicators in display zones which are either 67 or 100 metres long depending on the total length of the perimeter monitored by GUIDAR. The display shown in Figure 4 indicates a simple square perimeter. However, a display is made up for each site in which the string of alarm lights is made to represent a map of the perimeter. Such a site is shown in Figure 5. This is a GUIDAR unit used at Joyceville Penitentiary near Kingston, Ontario, Canada. The layout of the buildings is indicated in white on the black plastic face. The guard operating the GUIDAR unit is in voice communication with armed guards in towers around the perimeter. The guard can identify locations on the perimeter either by local description, for example, "north of the machine shop," or by the label on the display assigned to each display zone.

The processor is capable of detecting multiple targets if their separation exceeds two range cells. Therefore, it is possible for two adjacent alarm indicators to flash declaring multiple intruders. If intruders cross within a distance of two range cells from each other, they cannot be resolved by the processor anyway. Therefore, the ability to resolve or distinguish the presence of multiple targets is not impaired by lumping two or three range cells into one display zone. However, the uncertainty in the location at which an intruder crossed is increased from 33 metres to either 67 or 100 metres. This potential reduction in capability has been considered small because an intruder can move more than 50 metres by the time men can be deployed to that part of the 2 mile perimeter.

Alarm Assessment Capability

The GUIDAR display described above is on the unit which we currently have operating at several installations. The unit as described is straightforward to operate and the alarm display can be readily interpreted with very little training. However, there is information available that could be used by the operator to assess the alarm condition, and this information is not being presented by the present display. Before we go into this, perhaps a little background is in order.

The operation of a perimeter security system is divided into three distinct phases: detection, assessment and apprehension. In practice, electronic surveillance sensors such as GUIDAR/PCCS are used to provide detection of intruders. The probability of detecting a human intruder (P_D), the nuisance alarm rate (NAR) and the false alarm rate (FAR) are essential measurements of the sensor performance. While a good quality sensor has a high P_D and low NAR and FAR, one must assume that there will be some nuisance and false alarms. Hence only an alarm is raised then one must assess the alarm to determine if it is legitimate or not. The reliability and time response of the assessment procedure is a measure of the quality of assessment. Clearly if the nuisance or false alarm rate of the sensor is too high and/or the task of assessment too time consuming or unreliable, then the total security system is jeopardized. The prospects of a timely apprehension of the intruder are in essence determined by the quality of the detection and assessment capability.

The problem of target assessment becomes increasingly more difficult with perimeter length. In the case of human observers in guard towers the cost becomes prohibitive with long perimeters. Likewise the ust of CCTV is cost prohibitive due to the large number of cameras and the cost of lighting. In addition, the reliability of TV cameras, particularly in outdoor applications, is a major factor in life-cycle costs. In both direct human surveillance and CCTV surveillance, the effectiveness of target assessment is very dependent on visibility conditions; a vulnerability which is obvious to an intruder.

Available Data

When an intruder crosses the transducer (pair of leaky cables) information which is not used by the display could improve on the abi'ity to detect the target or to assess the nature of the target. The kinds of information suitable for alarm assessment are as follows:

- amplitude
- rate of change of amplitude
- phase
- rate of change of phase
- target width

The amplitude is the size of the return signal from the target which is a measure of his size. It is the nature of a detection system to provide a user with a simple yes/no declaration. The target is either there or it is not. However, it might occur that several targets cross at the same time or a single large vehicle crosses, appearing as one large target. In these cases the magnitude of the target is useful information. The rate of change of amplitude is a measure of how fast the target is crossing. Phase is a parameter that increases with distance along the perimeter. Of itself, it is not all that interesting. If a target moves away from the transmitter between the two cables, every time he moves two metres his phase will increase by 360°. Therefore, given the range cell of a target and his phase, one can have a target at any one of a multitude of locations (16) over the 33 metre range cell each spaced 2 metres apart. Therefore the phase itself is not all that interesting. However, the rate of change of phase tells us whether the target is moving away from or towards the transmitting end of the transducer. In addition, if several intruders cross at the same range cell together (i.e., one right after the other, or in a mass) the phase will jump around in a manner that does not happen for an individual intruder. With the existing display, whether several dozen intruders cross together or a single intruder crosses, one indication light for a display zone flashes. So, the operator cannot distinguish between the two cases. Another piece of available data is the width of a target. This may sound like a misnomer. The width of a human is of course about two feet. However, the return from an individual is blurred by the pulse over an effective distance of some 200 feet or about two range cells. Therefore, a plurality of intruders running across the cable, 20 feet or so apart, do not appear to the GUIDAR processor any wider than one target. Nevertheless, situations can occur in which say, two intruders cross the transducer at the same time, but separated by a distance of a few hundred feet. They become blurred by the pulse and if they are not too far apart will appear to the processor as one very wide target.

What we have then, is information relating to intruder alarms which can be used to improve detection and target assessment. What is to be done with these data? One could build a sophisticated pattern recognition system that is capable of classifying targets in the manner described above and present the description of results to the operator. The art (or science) of pattern recognition has been actively pursued since about 1957. In its earlier years, great enthusiasm and optimism prevailed that anything humans can do, machines can do also. Although in principle this may be true, in practice it is difficult to build a pattern recognition system that does complicated pattern classification and/or pattern description. Invariably, complications arise and usually two things occur: there are far more "bugs" to get out of the system than anticipated, and as fast as one bug is fixed, several new ones appear. A preferred approach, at least in our case, is to build a hybrid system using the high speed signal processing capabilities of the electronics and the powerful pattern recognition and training capabilities of the human brain. The objective is the presentation of data in such a manner as to stimulate the interest of the operator, yet not to annoy him with complicated instructions and interpretation.

Assessment Display

The practical application of an assessment display with GUIDAR/PCCS must be considered in determining the medium for such a display. The fastest moving intruder (7 metres/second) is only detected for approximately 250 milliseconds if he crosses the transducer at right angles. At the other extreme the slowest intruder (.02 metres/second) is detected for 100 seconds or more if he crosses in a diagonal direction. The GUIDAR/PCCS detection algorithm alerts the operator virtually instantaneously as the intruder approaches the first cable. The audible alarm associated with detection attracts the operator's attention. (In a good sensor the nuisance alarm rate/false alarm rate (NAR/FAR) is so low that operator vigilance is a serious problem.) In view of the very short duration of the high speed intruder, the display must involve some storage capacity. On the other hand, the operator must make an assessment quickly (say within 25 seconds) if a legitimate intruder is to be apprehended. These practical timing constraints virtually dictate that the display be of a television monitor type: a paper output such as used in sonar LOFAR-grams produces too much paper when processed at the required data rate.

The following television raster display is proposed as an optional assessment display fcr GUIDAR/PCCS:

a) Each line represents approximately 100 milliseconds of output data, the most recent at the bottom of the display with the past 50 seconds of data displayed vertically.

b) The horizontal axis is divided into 48 divisions, one for each cell (corresponding to one mile of cable) starting with the first cell on the left to the last cell on the right. Within each division there are 16 subdivisions corresponding to 22.5 degree phase angle increments.

c) The intensity of the display is controlled by target amplitude (A) to threshold (T) ratio. Six intensity levels are suggested,

Level	A/T
1	0 - .5
2	.5 - 1.0
3	1.0 - 2.0
4	2.0 - 4.0
5	4.0 - 8.0
6	8.0 - ∞

where level 1 is of least intensity and 6 is of greatest intensity.

All parameters presented in the above description are only suggested values. It is likely that these values will be altered based on experience.

Assessment Display Operation

The display technique described in the previous section does present the operator with all the basic target information available in GUIDAR/PCCS. In essence, the TV raster would be completely speckled without any perceivable patterns if the intensity were turned up and no targets were present. Targets will appear as patterns of lines on the TV raster. The vertical length of the lines correspond to the speed of crossing; the number of parallel lines to the physical length and size of the target, the intensity of the line to the target size and the slope of the lines to the along line velocity of the target. This is best illustrated by a few examples:

a) A Fast Crossing - A human travelling at 7 metres/second at right angles to the sensor cables (Figure 6a).

b) A Slow Crossing - A human travelling at .02 metres/second at right angles to the sensor cables (Figure 6b).

c) A Diagonal Crossing - A human travelling at .5 metres/second at 45° angle to the sensor cable directed away from the start of the cables (Figure 6c).

d) A Longitudinal Walk - A human travelling at .5 metres/second along the cable length towards the start of the cables (Figure 6d).

e) Simultaneous Crossings - Two humans travelling at .5 metres/second at right angles to the sensor cables but separated by a few feet (Figure 6e).

f) Burst of RF Interference - A lightning strike affects all cells simultaneously (Figure 6f).

Other patterns will be generated by environmental effects such as rainfall. These patterns will tend to fill the entire screen area in a somewhat random herringbone structure. These will be far larger in vertical and horizontal size than are legitimate targets.

Summary

The assessment display described in this paper presents a totally new approach to assessment of intrusion alarms. In practical terms it represents an optional add-on unit to be used with GUIDAR/PCCS. It offers several distinct advantages over traditional human or CCTV surveillance: (1) lower cost; (2) not dependent on obvious environmental conditions; (3) integrates the operator more closely with GUIDAR/PCCS. The effectiveness of the operator to make reliable assessments will only be determined by experience.

References

[1] Harman, R. K. and Mackay, N.A.M., "GUIDAR: An intrusion detection system for perimeter protection," Carnahan Conference on Crime Countermeasures, 1974.

[2] Clarke, D., Harman, R.K., Mackay, N.A.M., Reardon, C.R., "GUIDAR buried line sensor evaluation," Proc. of Carnaham Conference on Crime Countermeasures, Oxford, England, July 1977.

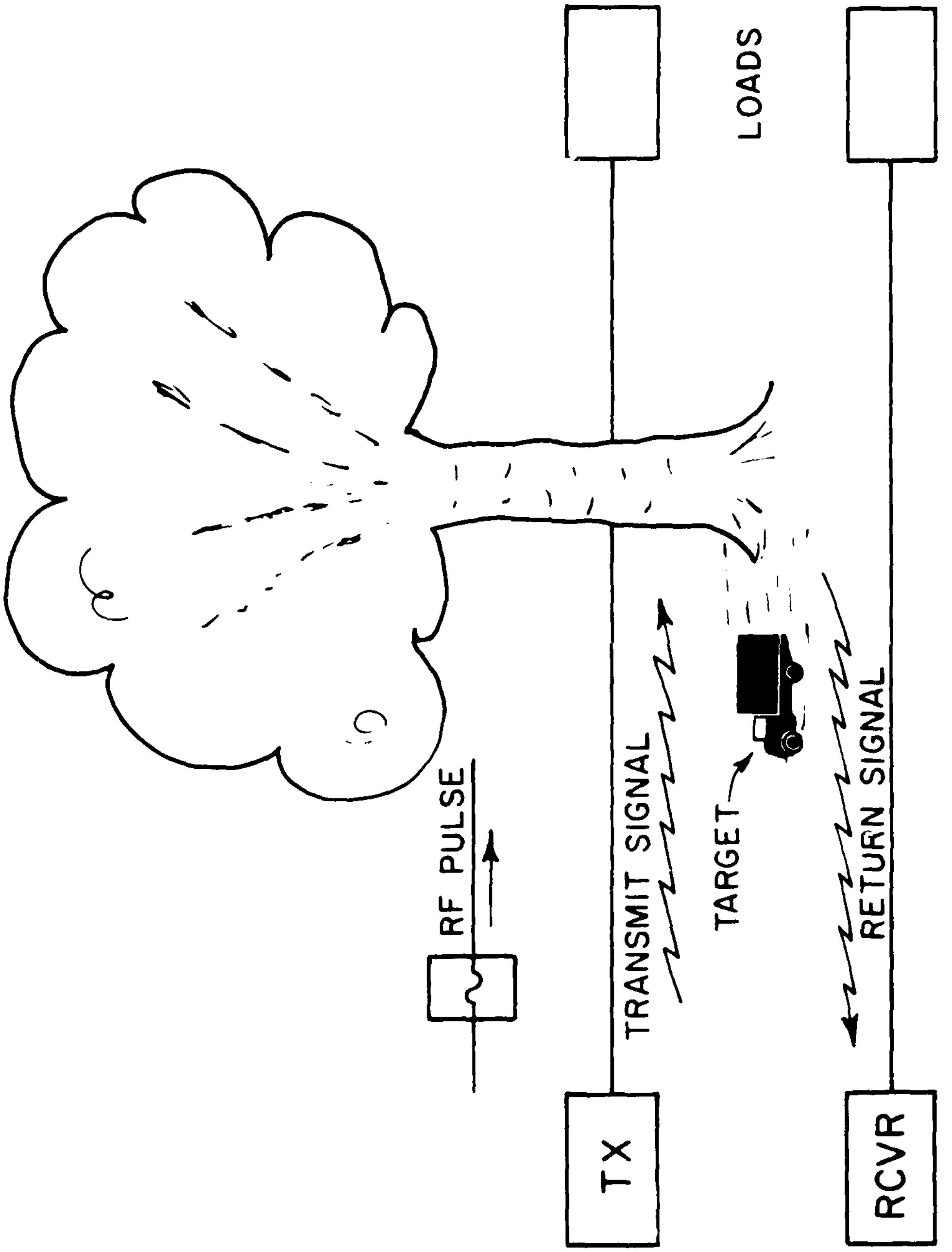


Figure 1. Guided Radar Concept

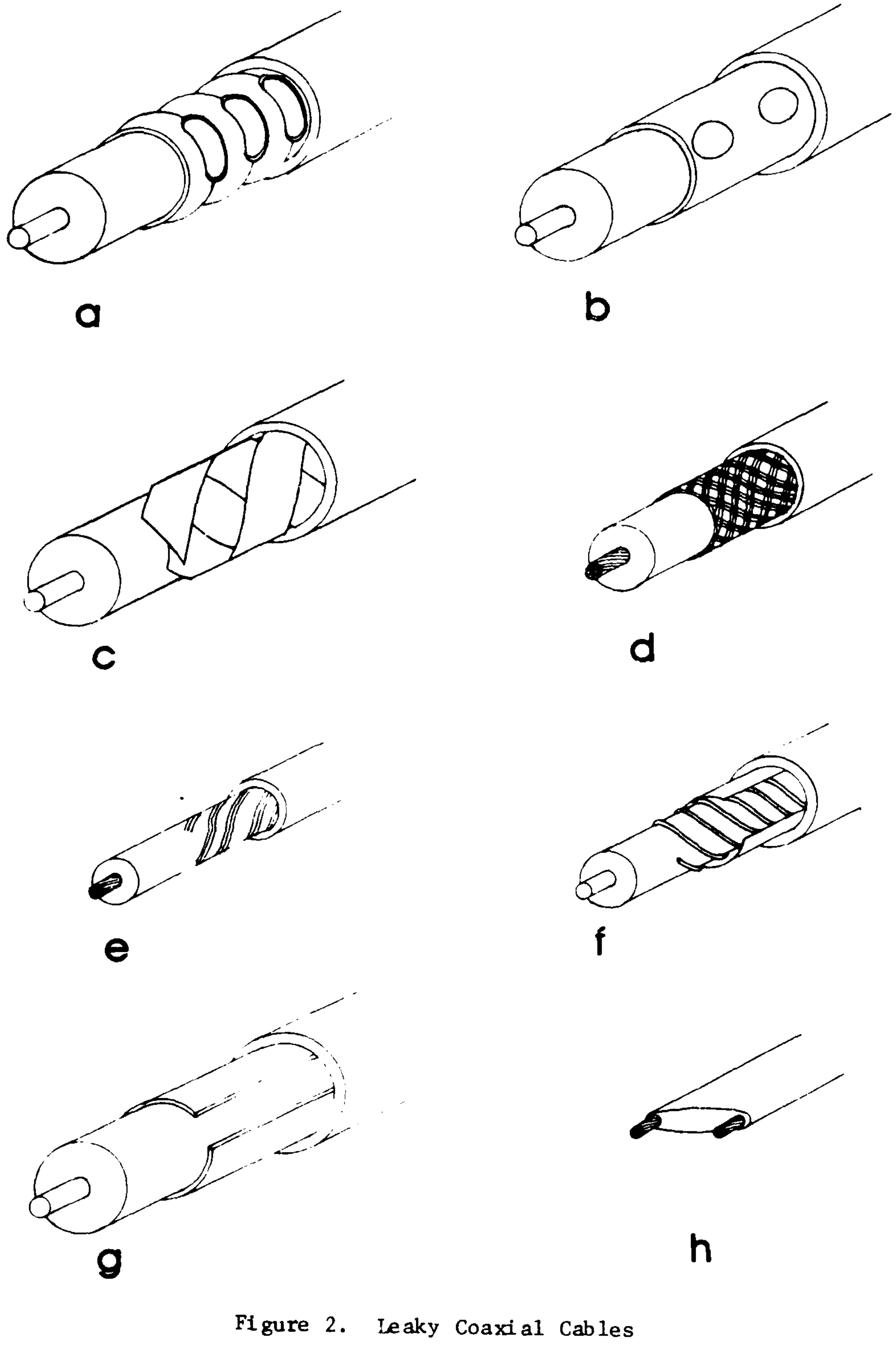


Figure 2. Leaky Coaxial Cables

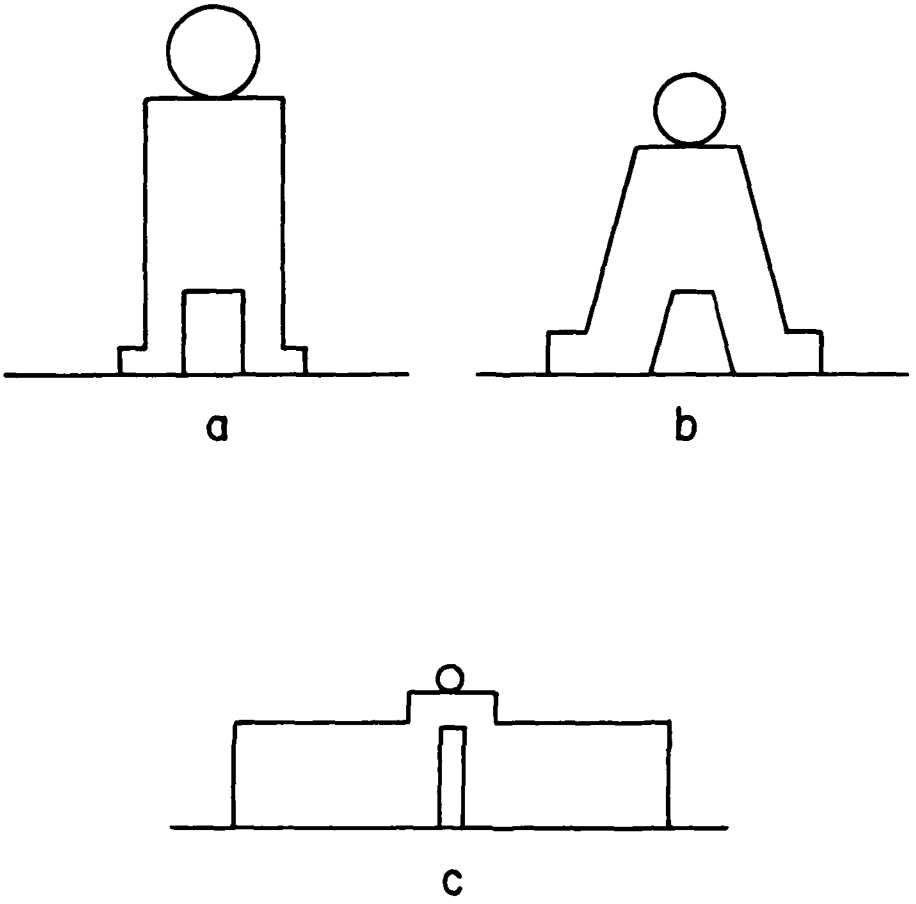


Figure 3. Apparent radar cross-sections. Equivalent free space radar cross-section for the same area and equal target reflection coefficients. 3a Uniform field. 3b Ported cables below ground. 3c Ported cables below high dielectric ground. Here the field is concentrated near the ground.

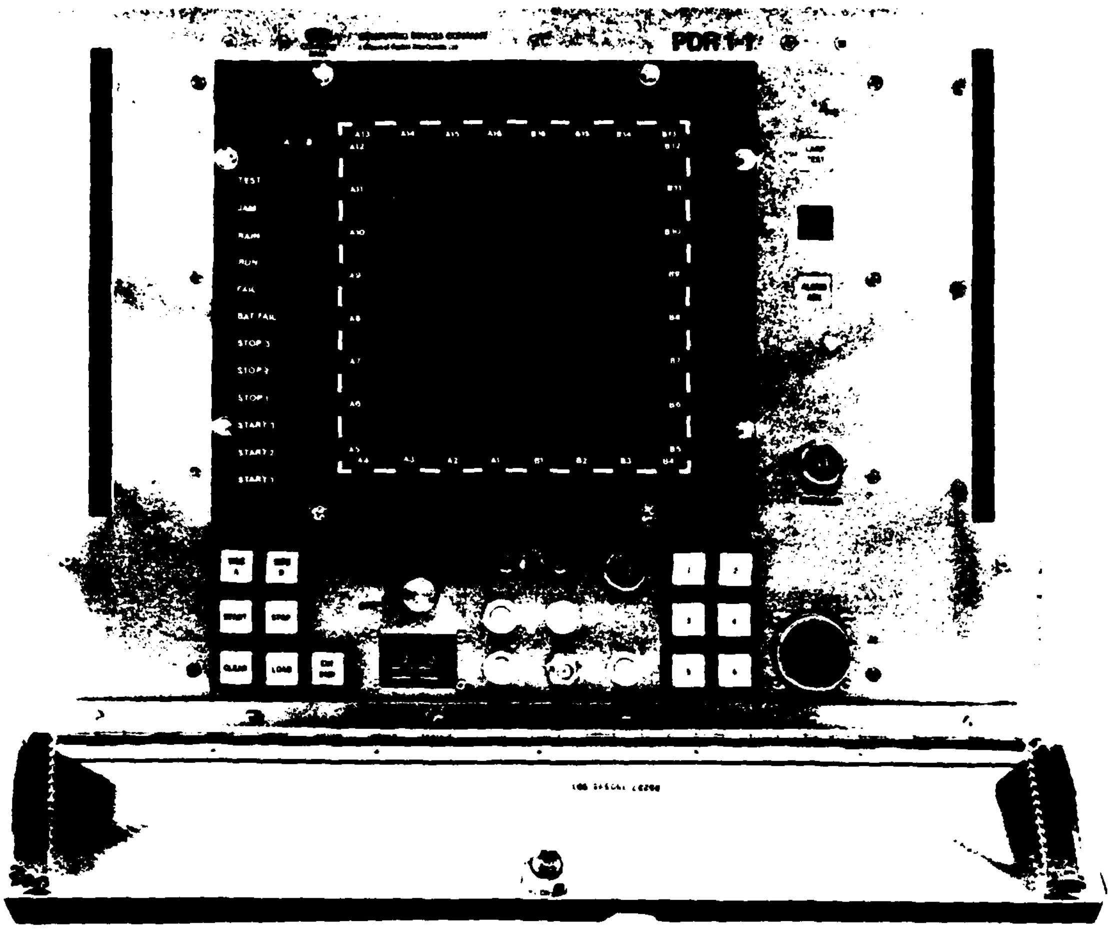


Figure 4. Processor, Detection and Ranging Unit (PDR 1-1)

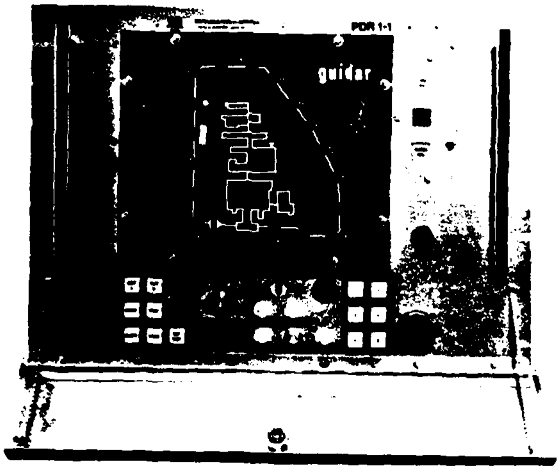
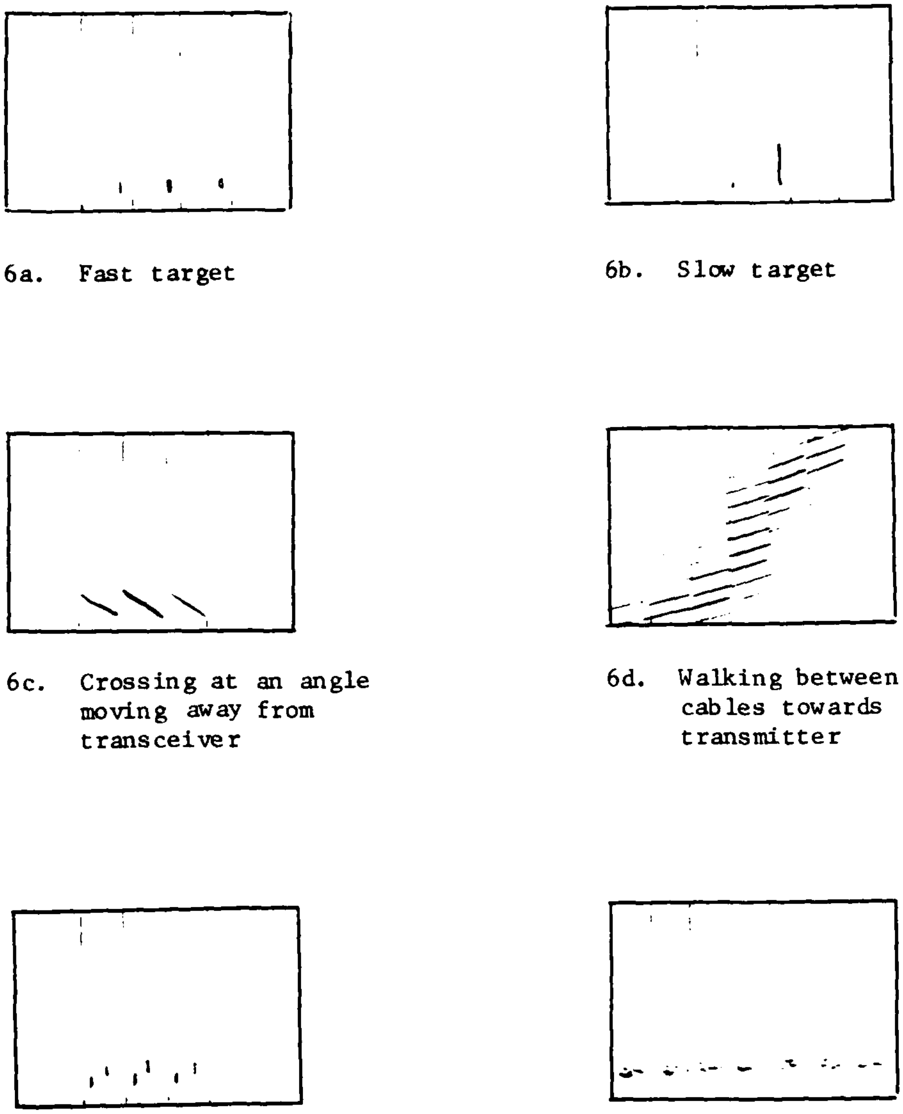


Figure 5. PDR 1-1 Custom Display



6a. Fast target

6b. Slow target

6c. Crossing at an angle moving away from transceiver

6d. Walking between cables towards transmitter

6d. Two targets crossing close in time, same cell, different phase

6f. EMI

Figure 6. Sample Alarm Assessments

DISCUSSION

QUESTION FROM THE FLOOR: Do you use a time built system for detecting the location of the individual along the cables?

MR. CHALMERS: No, we do not. We use TDR sets to determine whether or not the cable was broken when we are not using the system. But any pulse radar can be compared to a TDR. What we do is transmit a pulse.

Down the cable, we get a very weak return signal of noise. Due to the high pulse repetition frequency, based on the range length of the transducer, we do a lot of signal processing in order to get a high signal-to-noise gain. So, it is not simply a TDR; but it is quite similar.

QUESTION FROM THE FLOOR: How about the effect of conductivity of the soil on the operation of the system?

MR. CHALMERS: The conductivity of the soil has an effect on the sensor. We have had problems at one site in which they have a type of clay on which they have used a defoliant. We found that the sensitivity is low at this site. However, the variations in the sensitivity are accommodated either by the variations in the pulse power, which ranged from 200 to 800 miliwatts (a very low power level), or by the automatic threshold setting, when the guard walks around the perimeter to calibrate the system.

QUESTION FROM THE FLOOR: I was curious about how you were able to determine the appropriate sensitivity.

MR. CHALMERS: It is chosen to get the maximum probability of detection for the smallest target--the 75 lb target--and minimize the false alarm or the nuisance alarm rate for the 10 lb nuisance alarm.

It is just obtained by going through the sensitivity curve--as it falls off, it is a function of target mass and picking something somewhere in between.

OVERVIEW

Lt. Col. Gerald Williams
OASO, Defense Nuclear Agency
Washington, DC 20305

DNA is the oldest of the defense agencies. It began with the "Manhattan Project" in 1942 which developed the original "A" bombs dropped on Japan.

For the past two days you have heard various speakers talking about behavioral research projects and needs, and a few have discussed programs being funded by DNA. Today I will give you a quick overview of other physical security research projects not previously discussed.

Our mission is to conduct the Department of Defense nuclear weapons effects research and test program, to advise and assist on nuclear weapons matters throughout the Department of Defense, and to manage the nuclear weapons stockpile. DNA is also the integrated material manager for nuclear ordnance items.

To carry out our mission DNA is organized with several diverse and dispersed elements. You may have seen the headquarters element here on Telegraph Road.

At Bethesda, Maryland, is the Armed Forces Radiological Research Institute (AFRRI) which is our laboratory for conducting research in the field of radiobiology and related matters essential to the support of not only the DNA mission, but also the medical departments of the Department of Defense.

Field Command, the largest of DNA's subordinate organizations, is located at Kirtland AFB, Albuquerque, New Mexico. It performs many nuclear related functions in support to the DNA mission. Its location, in the heart of the nuclear community, is ideal. The Field Command, in coordination with the DOE, executes DNA's underground nuclear test program.

This close proximity to DOE field offices, Los Alamos scientific labs, Sandia Laboratories and other nuclear related functions such as the Air Force Nuclear Surety Group, Air Force Weapons Laboratory, and the Naval Weapons Evaluation Facility enhances close coordination of efforts beneficial to all.

Other major field command functions include weapons effects research, technical inspections of the services nuclear capable units and operation of the joint nuclear accident coordination center (JNACC).

Johnston Atoll is the primary U.S. overseas nuclear readiness to test facility. DNA, through Field Command, maintains a small personnel force there to insure readiness. DNA additionally is host to the Army for storage of their red hat munitions--(chemical agents removed from Okinawa), and a Coast Guard Loran station.

The Joint Nuclear Accident Coordinating Center (JNACC), in conjunction with DOE as its civilian counterpart, maintains current information on the location and availability of specialized DOD and DOE teams capable of responding to accidents involving radioactive materials.

o receives notification of accidents and requests for assistance

o requests appropriate assistance from DOD or DOE teams

o coordinates teams transportation

o obtains and relays information on the particular radioactive material involved.

In performing our mission, our relations throughout the Department of Defense and the nuclear community are broad and varied.

The Secretary of Defense supervises several DNA functions through designated deputies.

The Under Secretary of Defense for Research and Engineering supervises our nuclear weapon effects research and test program.

In certain specific areas, the Joint Chiefs of Staff exercise primary staff supervision over our activities.

The Assistant to the Secretary of Defense (for Atomic Energy) supervises our activities in areas such as technical nuclear safety and the logistical aspects of nuclear weapon stockpile management, applications of nuclear energy in non-weapon areas, DOD/DOE agreements on nuclear matters, and nuclear weapon security policy.

Specific DNA functions require close liaison with the DOE and its subordinate organizations. In many matters DNA is the single point of contact between the DOD and DOE.

Finally, DNA is the central DOD agency providing nuclear weapons support to the services, the commanders of the unified and specified commands, and other DOD and government agencies.

The threat to nuclear weapons has always existed; however, since the tragic Munich incident in 1972, conviction of two VEPCO employees for fuel rod sabotage, and the recent hijacking of a French train carrying irradiated fuel, the public perception and acceptance of that threat have increased significantly. Additionally, greater numbers of less-stable countries are developing nuclear capabilities albeit peaceful in nature. These factors, with congressional criticisms acting as catalyst, have spawned a major and coordinated effort within the Defense Department to improve and upgrade nuclear weapons security.

DNA's role in nuclear security has evolved into three major areas:

1. Nuclear security standards and criteria.

2. Advice and assistance to OSD/JCS.

3. Management of exploratory development.

Tasking by the Assistant to the Secretary of Defense for Atomic Energy and the Chairman of the DOD Physical Security Review Board has resulted in publication of a nuclear weapon security manual (NWSM). This document, based on the broad policy guidance in DOD Directive 5210.41, contains criteria and specifications for nuclear weapon storage areas as well as maintenance and alert facilities.

Advise and assist are very broad and all encompassing terms and likewise, require a variety of responses.

1. We participate in a variety of working groups such as the:

PSEAG - The executive agent for USDRE in his task to manage all security equipment procurement for DOD.

SEIWG - Subordinate to PSEAG attempting to insure operability and compatibility between various types of equipment.

TSRWG - The group that develops formal requirements documentation which drives equipment development.

2. We have sponsored symposia and conferences such as the Joint Services Nuclear Surety Conference, and several behavioral science symposiums.

3. Special projects include:

- FIDS/BISS/commercial/NATO analysis was in response to Congress and USDRE to confirm and quantify the duplication alleged to exist in the security equipment development field.

- LRSP support will be addressed in some detail later.

- Progress assessment (ATSD(AE)) is an attempt to measure the progress of the total Army upgrade program some four years into the effort.

One of the most challenging and essential security functions performed in conjunction with the services, involves DNA's site security basic research program. This effort had its beginning in FY 1974 with a few O&M dollars utilized to conduct some basic evaluation of fencing and barrier materials being considered for standardized use throughout DOD.

We looked at a combination of barriers and fence applications. The results indicated that a fence was only a boundary and no more than a minor obstacle to the terrorist overt threat. The actual tests, findings, conclusions, and recommendations accruing from this basic effort resulted in cost avoidance decisions of approximately $73 million. It was obvious that similar RDT&E ventures related to physical security were necessary.

Since that initial, modest effort, our budget has progressed to nearly six million dollars. Initially our goal was simply to acquire scientifically valid data for the development of optimum security systems.

However, in 1977, USDRE tasked DNA to conduct, in cooperation with the services, all exploratory development which has application to nuclear security.

DNA manages all nuclear security equipment exploratory development efforts, and passes on to a specific service those efforts which should be entered into advanced development. This arrangement permits tri-service participation in a single R&D program, designed to eliminate duplication.

Research (6.1) - Defense-related research, through in-house laboratories and contractual support, in a continuous search for new scientific principles or concepts related to long-term national security needs. It provides fundamental knowledge for the solution of identified military problems and furnishes the base for subsequent exploratory and advanced developments.

Fxploratory Development (6.2) - Includes efforts to determine how to apply scientific principles toward the solution of broadly defined problems, short of major development programs, in order to develop and evaluate technical feasibility.

Advanced Development (6.3) - (A) Identification of alternative concepts as potential solutions to mission needs resulting in brassboard demonstrations, not operational systems (milestone 0). (B) Application of new technology by developing hardware for demonstration and validation for test and proof of concept (milestone 1).

Full Scale Engineering Development (6.4) - Includes those systems which are determined to have priority application for integration into the force structure and are being engineered for service use (milestone 2).

Management & Support (6.5) - Includes efforts directed toward support of installations or operations required for use in general research and development.

Several of the principal investigators have already spoken on their efforts so I won't attempt to amplify.

We are conducting analyses of existing research in areas related to psychologically repelling phenomena. These efforts seek to evaluate the effects on humans of various deterrents (e.g., barriers, fencing, lighting, guard force) and new concepts and devices as they are developed. These studies will form the basis for exploratory research programs to expand and improve deterrence as an adjunct to physical security.

We are conducting basic research in areas related to human behavior and response phenomena vis-a-vis a wide variety of security stimuli and environments. Among other things, we are trying to develop research programs to investigate vigilance and establish taxonomy based on:

1) Individual differences,
2) Design of data displays,
3) Design of tasks,
4) Watch scheduling,
5) Function allocation,
6) Environmental conditions.

Such research may also be helpful in determining optimum security personnel selection and retention criteria and provide motivation techniques for security personnel to diminish inherent boredom and tedium phenomena.

Another behavioral project is our candidate assessment study which is being coordinated with the U.S. Army Military Police School. The effort will determine what behavioral factors influence personnel performance and are identifiable before assignment to nuclear security duties. The research has included development of job analyses which are providing necessary training development data for the MP school. The research has provided a significant behavioral assessment of MP utilization in nuclear security. The many recommendations are currently being reviewed for possible implementation or test. Meanwhile, the project is currently examining individual MP's perception of the threat to his or her site and the resulting impact on job performance. Data concerning the probability of an MP becoming an insider threat is also being gathered.

Also a behavioral science investigation, our "Comm Paradign" attempts to scrutinize human behavior through a minute analysis of the information which passes through the sensor/communications network of an operational site. This work, headed by the emminent Dr. Robert Mackie, attempts to clearly identify man-related strengths and weaknesses of our security systems including those deficiencies precipitated by the man-machine interface. Dr. Mackie identified the program as SSOPRA.

The Law Enforcement Standards Laboratory of the National Bureau of Standards has been investigating various techniques to "tag" individuals who penetrate exclusion areas, and subsequently trace them to facilitate recovery or prosecution. Two particulate tags will be transferred to 6.3 in FY-81. Exploratory development of gaseous taggants and long distance (up to 1 km) trace detectors is continuing. Ultimately, NBS expects to identify a gaseous tag which will be inhaled by an intruder, metabolized, and excreted via breath and skin over a period of several days.

It is commonly assumed that once an individual penetrates an alarmed perimeter, he is easily tracked and engaged by responding forces. Not so, particularly during periods of reduced visibility, intruders can wander freely about most large storage areas until they activate another alarm at the storage structure, if in fact, that is their intent.

We are exploring the practicality of adapting line-of-sight microwave perimeter sensors to area coverage using multiple frequencies, omnidirectional transmitters, and bandpass filtered receivers. If we can develop a system complete with microprocessor/correlator that will work around fixed obstacles and terrain anamolies, we will have a system for tracking intruder(s) to insure a rapid response and a favorable engagement.

Exemplifying 6.2 research, is our project to develop a negative ion intrusion detection system for interior areas. The concept involves generating a steady-state dc current and a flow of ions through a structure and measuring the reduction caused by a human presence. Theoretically free from false alarms caused by other sensors, environment, or EMI, the technique promises a quantum leap forward in the area of interior sensors.

"Tunnel conduit" is a program to develop sensors which will detect electronics emplaced in electrical or other types of conduit surrounding critical resources. Among other uses, it may serve to santize future MX sites to assist in the preservation of location uncertainty a concept which is so essential to MX deployment.

I said earlier that I'd try to avoid repetition; however, even though several speakers have touched on this area they have not conveyed the intensity of DNA/SONS concern over this nuisance alarm monster. So for what its worth, here is the DNA position. Historically, intrusion detection sensors have had a high degree of reliability--they don't miss many penetration attempts. Unfortunately they are as adept at detecting tumbleweed, cattle, squirrels, and rabbits as they are man. DNA is sponsoring and consolidating several efforts to develop systems that will process the analog data received by sensors to "learn" what man looks like, screen and reject all other signatures, and transmit only the digital data necessary to advise the alarm monitor that a person has penetrated the field of the sensor. These systems are known variously as distributive smart, and adaptive processors.

The study of lightweight ballistic resistive materials attempts to develop specifications and standards for various configurations of flexible materials to protect ordnance, guard posts, transportation vehicles, etc., that are subject to small arms attack. The armored blanket, shown here, has been passed to the field command for field validation. You see it being emplaced, alertly waiting for some red hat to attack it, and successfully thwarting the villan.

In firing demonstrations, the blanket performed better than anticipated, defeating bullets up to 7.62 mm AP with one layer and projectiles up to 23 mm HEl with two layers.

The final prototype blanket design consists of slats of two kinds of armor bonded to Kevlar mats. The blankets tested were approximately 2 in thick and measured 30 in by 56 in and weighed approximately 128 lbs each.

NBS is also conducting measurement tests on various materials to quantify fracture resistance, stress behavior, and ability to dampen propagation of impact waves. As a spinoff, they have developed a "Winsor probe gun," which fires a probe at a measured velocity into concrete. By extrapolating the measured penetration, the resistance of the tested material can be estimated.

We are supporting metallurgical research for enhancing barrier material and refining fabrication techniques for casting irregular particles of aluminum-oxide or similar high density materials in aluminum magnesium alloy.

Conceptually, the computerized site security monitor and response system is visualized as a network in which all site security systems, including intrusion detection equipment, duress alarms, guard radio, and telephone systems, etc., are interfaced to a tripley redundant computer to provide timely, accurate and unambiguous information about the progress of an attack or intrusion attempt. The system will also provide and implement programmed decisions of how best to counter the threat. Automatic upchannel status reports will signal any change in site security status and the response actions which are being initiated.

LTC Rinehart mentioned, in his welcome yesterday, that his staff had assured him there are four essential elements of security but we couldn't identify them. Another way of saying that is that the industry has pointed research toward quantitative answers--but we don't know the proper questions yet. Even though we call our locations restricted areas, we do not know which of the measures indicated is most effective, either singly or in combinations, in providing protection. We do not know how to quantify the value of a fence, a light, a lock, a man with a M-16, etc.

This is the purpose of this project, a necessary step toward implementation of a physical security system analysis methodology.

A long term goal of our agency is to develop a test site. A site where testing of equipment, procedures, and people can be accomplished in a "full-up" completely operational environment. That is, with real people, real weather conditions, real attack or penetration scenarios. This current effort, a first step toward that goal, involves scoping and quantifying what the technical and electronic requirements will be in order to accomplish our goal.

This is an initial investigation of the feasibility of using an Army driver training technique for nuclear weapons security. Multiple video frame photos are pre-recorded and stored on the floppy disc of a computer. The computer is in turn connected to a control device to allow individuals to "drive" into a site and structures thereon without ever approaching the real site. The application of this technique to recovery or recapture efforts could be significant.

In response to growing concern over duplication of hardware development, and a lack of interoperability between various hardware items, DNA has embarked on the integrated security system. It is an attempt to provide a nuclear weapons security development program culminating in a complete system in the post 1990 time frame, integrating all elements into a systematic and coordinated approach.

- Weapon Systems Characteristics
  - o Pershing, Artillery, Fighter/Bombers
- Weapon Systems Configuration
  - o In Storage, in Convoy, Deployed Alert Posture
- Posture
  - o Peacetime Transition/War
- Evolutionary Phasing

In support of the Army upgrade program in Europe, we enlisted the aid of experts from Sandia National Labs to monitor technical aspects of sensor hardware installation. They have set up a mock NATO site in New Mexico and have made some significant contributions toward identifying and avoiding problems, developing specifications, and generally assisting with the program.

We discussed DNA's role in the nuclear weapons security exploratory research program a moment ago. What you have just seen is that portion of the program that DNA manages directly. What you are about to see is that portion of the program that the services manage using DNA 6.2 money. We obviously 'manage these efforts also, but only in the broader sense of exercising veto power over those which are duplicative or unpromising.

As mentioned earlier, we have sponsored diverse investigations into barriers and their penetrability. This one specializes in combinations of various metals, alloys, and laminates and application of the latest techniques of penetration--jet ax, pyronol, and power saws--to attempt to defeat them.

This is a two phase project as indicated:

o Develop miniature low light level CCD-TV camera with sensor package of one cubic inch.

o Develop analog low light level moving target sensor for automatic intrusion detection.

Regardless of the effectiveness of barriers and associated physical security equipment it is anticipated that manned forces will continue to be a major essential element in the protection of facilities. Inasmuch as eye acuity is a principal sensory function, but is relatively poor in humans under low ambient light levels, illumination factors are most important in areas where protection is at least partially dependent upon human observation.

Explosive detection has applications ranging from bomb squad use to preventing the introduction of contraband explosives into nuclear weapons storage areas. While our canine friends have helped us many times, a "black-box" detector is easier to carry around, cheaper to feed, and does not have to have its kennel cleaned out daily. This research effort has developed a TNT enzyme which catalyzes with molecules of TNT in the atmosphere surrounding explosives in a biochemical reaction. That reaction is chemically coupled to a light emitting indicator who's fluctuations can be measured by photo multiplier equipped instruments and can thus trigger an alarm.

The locking system utilized to secure most nuclear weapons storage magazines, consists of a high security padlock attached to a surface-mounted high security hasp. This basic approach, while utilizing modern materials and manufacturing techniques, is representative of the state-of-the art in the 19th century and unnecessarily exposes the lock and the locking hardware to forcible and surreptitious entry, attack, sabotage, and the rigors of the natural environment. Such systems are rapidly neutralized by the use of force and are prone to malfunction and/or lockouts due to the effects of corrosion, dust, and freezing weather. Further efforts to develop better padlocks and hasps will not significantly improve the situation. The development of new concepts for locking mechanisms and locking hardware that are located inside the protected area could result in a five or ten-fold increase in forcible entry denial time when installed in an adequate entrance closure.

As such, the Navy is undertaking the locking effort for DOD.

A long term project which seems to get attention and support only during incidents such as the Pueblo and, more recently, the takeover of an embassy, anti-compromise emergency destruction systems (ACED) are being developed by the Naval Ordnance Station, Gun Systems Division. System design criteria include option for intruder or command activation, destruction of 99.9 percent of material, and time lines such as 5 min aboard aircraft, 30 min aboard ship, and 1 h on land.

The Navy's fleet, for all the emerging technology, is still largely pre-1970's vintage. Much of the communication on board is voice tube, or sound powered phone. To prepare for new ships and retrofit of old--where possible--Harris has looked at six communication systems and made some recommendations. First is to link intraship sensor data with fiberoptics using a simple algorithm to show the gross health of the cable. Coaxial is proposed as a video carrier, with short range rf links protected with voice privacy features, and long range satellite communication protected by the data encryption standard.

In this Buck Rogers era, it should not surprise anyone that we were reaching for some pretty exotic (far-out) ideas. One of these is visible light holography for possible uses in the shipboard security functions. The system would be used to hinder, delay and mislead intruders by providing realistic lifelike, visual, and IR illusions, including open area deception.

A quick effort this year is one that White Oak is doing for us to integrate physical security including nuclear into the ship's vital functions and design.

Computer modeling of combat engagements is not startlingly new. Neither is the practice of having proponents interact with one another in real time, changing tactics, troop location, and other factors as the engagement progresses. This technique has not, however, been developed for use with very small units in defense of nuclear weapons. We have sponsored a modest program with the Air Force to develop a small unit engagement graphics system that will treat these requirements explicitly. With this, they expect to be able to develop not only optimum tactics for each specific site; but, also to develop optimum tacticians.

This study, labeled Air Force Candidate Assessment, is essentially the same as the Army study. We anticipate that Abbott will identify significant differences between services and hopefully the causitive factors driving those differences.

The triaxial force sensor is a fancy name for describing a device which must sense some force being applied to a fence in three axes in order to alarm. The attempt, fairly successful to date, is to retain adequate P_d while dramatically reducing nuisance alarms. 6.3 next year.

The Physical Security Systems Directorate, in pursuit of its mission to develop exterior sensors for nuclear weapons storage has currently under development, the electret tape transducer, an ultrasonic device in tape form, which is intended to be easily applied to any reasonably non-porous surface. This transducer represents an addition to the Biss family of equipments for applications where a temporary easily-installed line sensor is desirable.

Current work in the area of IRCCDTV consists of a sensor with a single 256 element line array, and thus provides no two-dimensional imagery. With this effort the Air Force expects to extend the technology as indicated on this slide.

Control data presented their version of buried line sensors and some useful applications of the associated phenomena. RADC is exploring the feasibility of extending the useful detection zone into the wild blue yonder.

We have here an exploration of the potential to use leaky coaxial cable to track and classify intruders and to extend the detection zone upward to detect encroaching airborne personnel and vehicles.

The objective of the entry control program is to arrive at an optimum system configuration for a real world operational access control system.

Three verification systems, automatic speaker verification (ASV); automatic handwriting verification (AHV); and automatic fingerprint verification (AFV) have been built and individually evaluated.

The ASV system, as well as the other verification techniques, will form the menu for investigation and trade-off to configure a cost-effective system to minimize error rates and maximize throughput rate.

In addition, this effort will improve the currently developed automatic speaker verification (ASV).

The advanced system is based solely on an individual's voice patterns. The technique utilizes an automatic connected speech recognition system capable of recognizing the digits independent of speaker. The user simply speaks his code (6-digit number) and the machine automatically recognizes the code and uses the same speech information for verification.

This completes my presentation on "odds and ends.' It has been a distinct pleasure to address such an august group. Although the proportion of dollars which we allocate to behavioral work still falls short of our goal, we remain firmly committed to making physical security systems subservient to instead of dominant over, man. To enhancing his strengths and minimizing his weaknesses so that someday we can say that man is no longer the weak link in the system. Thank you very much.

Attendee List

Preston S. Abbott
Abbott Associates, Inc.
300 N. Washington St.
Alexandria, VA 22314

LTC David L. Adderley
U.S. Army Material Development
& Readiness Command
Headquarters
5001 Eisenhower Ave.
Attn: DRCSS
Alexandria, VA 22333

Joseph M. Albanese
Tracor, Inc.
1600 Wilson Boulevard
Suite 200
Arlington, VA 22209

Harris D. Arlinsky
U.S. Army Intelligence &
Security Command
Arlington Hall Station
Arlington, VA 22212

Robert L. Barnard
MERDC
Counter Det. Div.
Ft. Belvoir, VA 22060

Marvin Beasley
Defense Nuclear Agency
Washington, DC 20305

Patricia Benner
Mission Research Corp.
5503 Cherokee Ave., Suite 201
Alexandria, VA 22312

Frederic A. Bick
Effects Technology,
Incorporated
5385 Hollister Ave.
Santa Barbara, CA 93111

William D. Bitler
OASO
Defense Nuclear Agency
Washington, DC 20305

Larry K. Blankenship
JAYCOR
3001 Mountain Road Place, NE
Albuquerque, NM 87110

Daniel William Buehler
E-Systems, Inc.
Greenville Division
P.O. Box 1056, Majors Field
Greenville, TX 75401

C. R. Bukolt, CPP
HQ Naval Material Command
Attn: MAT 0462
Washington, DC 20360

Dr. Jerry J. Cadwell
Brookhaven National Laboratory
Building 197-C
Upton, NY 11973

Douglas R. Cavileer
NUSAC, Incorporated
7926 Jones Branch Drive
McLean, VA 22102

James Chalmers
Computing Devices Company
3685 Richmond Rd.
Bells Corners, Nepean, Ontario
Canada K1G 3M9

James Clifton
National Bureau of Standards
Building Research B348
Washington, DC 20234

Dr. Francis J. Cook
Adaptronics, Inc.
1750 Old Meadow Road
McLean, VA 22102

Michael F. Davis
JAYCOR
205 South Whiting St., Suite 607
Alexandria, VA 22304

James R. DeVoe
National Bureau of Standards
Chemistry A212
Washington, DC 20234

Clarence J. Douglas, Jr.
D&D Inc.

Joseph C. Drauszewski
SORD
Defense Nuclear Agency
Washington, DC 20305

David J. Duff
Sylvania Systems Group
GTE Products Corporation -
Western Div.
100 Ferguson Drive
Mt. View, CA 94042

Lawrence K. Eliason
National Bureau of Standards
Physics B157
Washington, DC 20234

Larry Ewing
Mission Research Corporation
P.O. Drawer 719
Santa Barbara, CA 93102

Brian H. Finley
Sandia National Laboratories
Division 1223
Albuquerque, NM 87185

Michael E. Fletchall
HQ USAMDW
Attn: ANOPS-LE-PS
Fort Lesley J. McNair
4th & P Streets, SW.
Washington, DC 20319

Daniel E. Frank
National Bureau of Standards
Physics B157
Washington, DC 20234

Gary Fuller
Aerospace Corp.
955 L'Enfant Plaza, SW.
Washington, DC 20024

Jennifer Gagnon
National Bureau of Standards
Metrology A353
Washington, DC 20234

Daniel Garges
Ensco

Howard C. Gerold
Naval Weapons Support Center, Crane
753 Sunset Drive
Bloomfield, Indiana 47424

Major David H. Gilmore
Defense Logistics Agency
Cameron Station
Alexandria, VA 22314

Clare Goodman
National Bureau of Standards
Metrology A353
Washington, DC 20234

John F. Haben
Naval Surface Weapons Center
White Oak
Silver Spring, MD 20910

Robert J. Hall
Contractor, Mission Research
Corp.
P.O. Drawer 719
Santa Barbara, CA 93102

Walter Charles Hernandez, Jr.
ENSCO, Inc.
5408A Port Royal Road
Springfield, VA 22151

Van D. Holladay
Cypress International
333 N. Fairfax St.
Alexandria, VA 22314

Mr. Joseph W. James
Nuclear Regulatory Commission
Mail Stop EW 359
Washington, DC 20555

Chester C. Jew
Office of Federal Protective
Service Management, PS
GSA Bldg., Room 2038
18th and F Streets, NW.
Washington, DC 20405

David P. Johnson
PME 121

Dr. Bert T. King
Office of Naval Research
800 N. Quincy St.
Arlington, VA 22217

Lawrence Knab
National Bureau of Standards
Building Research B348
Washington, DC 20234

Ernest A. Koehler
Navy Personnel R&D Center
(Code P302)
San Diego, CA 92152

Joel J. Kramer
National Bureau of Standards
Metrology A353
Washington, DC 20234

Samuel Kramer
National Bureau of Standards
Technology B142
Washington, DC 20234

Paul Krupenie
National Bureau of Standards
Physics B157
Washington, DC 20234

Quon Yin Kwan
Aerospace Corp.
955 L'Enfant Plaza, SW.
Washington, DC 20024

Robert D. Ladd
Nuclear Energy Services

George Lapinsky
National Bureau of Standards
Metrology A353
Washington, DC 20234

H. B. Leedy
U.S. Army Military
Personnel Center
200 Stovall St.
Alexandria, VA 22311

Dr. Gregory W. Lewis
Navy Personnel R&D Center
(Code P302)
San Diego, CA 92152

Patrick R. Lowrey
Cypress International, Inc.
333 N. Fairfax St.
Suite 201
Alexandria, VA 22314

Robert R. Mackie
Human Factors Research, Inc.
5775 Dawson St.
Goleta, CA 93017

Stephen Margulis
National Bureau of Standards
Building Research A355
Washington, DC 20234

Bruce P. Marion
GTE Products Corporation
Sylvania Systems Group - Western Div.
100 Ferguson Drive
Mt. View, CA 94042

Richard A. Mauldin
Industrial Security Defense
Logistics Agency
Cameron Station
Alexandria, VA 22314

Robert S. McGowan
JAYCOR
205 South Whiting St., Suite 607
Alexandria, VA 22304

Thomas J. Midura
Harold Rosenbaum Assoc., Inc.
40 Mall Road, Suite 207
Burlington, MA 01803

Rudy A. Miller
Sylvania Systems Group
GTE Products Corp. - Western Div.
100 Ferguson Drive
Mt. View, CA 94042

Robert Moler
Aerospace Corp.
955 L'Enfant Plaza, SW.
Washington, DC 20024

R. T. Moore
National Bureau of Standards
Technology A219
Washington, DC 20234

Randall Murphy
New York University
Dept. of Chemistry
New York, NY 10003

Joseph T. Nelson
USAF/RADC
RADC/IRAA
Griffiss AFB, NY 13440

W. D. Norman
New Zealand Embassy

James H. Ott
Battelle Memorial Institute
2030 M Street, NW.
Washington, DC 20036

Mr. Joseph W. Payne
JFKCENMA
G-3 Special Projects
Ft. Bragg, NC 28307

Daniel A. Perkowski
OANS
Defense Nuclear Agency
Washington, DC 20305

Julius Persensky
National Bureau of Standards
Metrology A353
Washington, DC 20234

Michael K. Pilgrim
Science Applications, Inc.
1710 Goodridge Dr.
McLean, VA 22102

Maj. Richard A. Pomager, Jr.
HQ DA (DAPE-HRE)
Washington, DC 20310

Ann Ramey-Smith
National Bureau of Standards
Metrology A353
Washington, DC 20234

William G. Rauen
Naval Surface Weapons Center
Bldg. 405, Room 220
Silver Spring, MD 20770

Donald R. Richards
Booz Allen Applied Research
4330 East West Highway
Bethesda, MD 20014

Barton B. Rinehart
OANS
Defense Nuclear Agency
Washington, DC 20305

Richard M. Rock
Center for Naval Analyses/
Navy
2000 N. Beauregard St.
Alexandria, VA 22311

Frederick Roder
Aerospace Corp.
955 L'Enfant Plaza, SW.
Washington, DC 20024

Joseph R. Rodriguez
General Services Admin.
Office of Security and Occupational
Safety & Health
18th and F Streets, NW.
Washington, DC 20405

Dr. Alexander G. Rozner
Naval Surface Weapons Center
White Oak
Silver Spring, MD 20910

Lonnie Sandy
HQ USAMDW
Attn: ANOPS-LE-PS
Fort Lesley J. McNair
4th & P Streets, SW.
Washington, DC 20319

Lorenzo Senires
Defense Logistics Agency
Executive Directorate
Industrial Security
Room 8B408, DLA-NI
Cameron Station
Alexandria, VA 22314

Frank Sevcik
RDA

Donald R. Shoemaker
R & D Associates
4640 Admiralty Way
P.O. Box 9695
Marina del Rey, CA 90291

Daryl K. Solomonson
Mission Research Corporation
5503 Cherokee Ave., Suite 201
Alexandria, VA 22312

William J. Stinson
Navy Personnel R&D Center
(Code P302)
San Diego, CA 92152

Marshall J. Treado
National Bureau of Standards
Physics B157
Washington, DC 20234

Charles Wallach
Behavioral Research
Associates, Inc.
1220 Blair Mill Road #1205
Silver Spring, MD 20910

Stanley I. Warshaw
National Bureau of Standards
Metrology B364
Washington, DC 20234

Gerald O. Williams
OASO
Defense Nuclear Agency
Washington, DC 20305

Theodore C. Williams
JAYCOR
205 South Whiting St., Suite 607
Alexandria, VA 22304

William J. Witter
SONS
Defense Nuclear Agency
Washington, DC 20305

Charles E. Wold
The BDM Corporation
1801 Randolph Rd., SE.
Albuquerque, NM 87106

DISTRIBUTION LIST

DEPARTMENT OF DEFENSE

Defense Logistics Agency
ATTN: L. Senires, DLA-NI
ATTN: R. Mauldin
ATTN: D. Gilmore

Defense Nuclear Agency
ATTN: NSRD, W. Bitler
ATTN: NSRD, G. Williams
ATTN: NSRD, W. Witter
ATTN: NSRD, J. Drauszewski
4 cy ATTN: TITL
20 cy ATTN: OPNS, B. Curtis

Defense Tech Info Ctr
12 ATTN: DD

DEPARTMENT OF THE ARMY

US Army Material Dev & Readiness Cmd
ATTN: DRXSS, D. Adderly

US Army Intelligence & Sec Cmd
ATTN: H. Arlinsky

US Army Milpercen
ATTN: H. Leedy

Hq USAMDW
ATTN: ANOPS-LE, L. Sandy
ATTN: ANOPS-LE, M. Fletchall

US Army, J.F. Kennedy Ctr (MA)
ATTN: G-3, Special Projects, J. Payne

Hq DA
ATTN: DAPE-HRE, R. Pomager

US Mobility Equip R&D Cmd
ATTN: Counter Det Div, R. Barnard

DEPARTMENT OF THE NAVY

Headquarters
Naval Material Cmd
ATTN: MAT 0462, C. Bukolt, CPP

Naval Personnel Res & Div Ctr
ATTN: Code P302, E. Koehler
ATTN: Code P302, G. Lewis
ATTN: Code P302, W. Stinson

Naval Weapons Support Ctr
ATTN: H. Gerold

Naval Surface Weapons Ctr
ATTN: J. Haben
ATTN: A. Rozner
ATTN: W. Rauen

Office of Naval Research
ATTN: B. King

Center for Naval Analysis
ATTN: R. Rock

DEPARTMENT OF THE AIR FORCE

Rome Air Development Center
ATTN: IRAA, J. Nelson

DEPARTMENT OF ENERGY

Associated Universities, Inc
ATTN: J. Cadwell

OTHER GOVERNMENT AGENCIES

Nuclear Regulatory Commission
ATTN: Mail Stop EW 359, J. James

General Services Administration
ATTN: PSSS, C. Jew

National Bureau of Standards
ATTN: Bldg Research, B348, J. Clifton
ATTN: Chemistry, A212, J. Devoe
ATTN: Physics, B157, L. Eliason
ATTN: Physics, B157, D. Frank
ATTN: Metrology, A353, J. Gagnon
ATTN: Metrology, C. Goodman
ATTN: Building Research, B348, L. Knab
ATTN: Metrology, A353, J. Kramer
ATTN: Technology, B142, S. Kramer
ATTN: Physics, B157, P. Krupenie
ATTN: Metrology, A353, G. Lapinsky
ATTN: Building Research A355, S. Margulis
ATTN: Technology, A219, R. Moore
ATTN: Metrology A353, J. Persensky
ATTN: Metrology, A353, A. Ramey-Smith
ATTN: Physics, B157, M. Treado
ATTN: Metrology, B364, S. Warshaw

General Services Administration
ATTN: J. Rodriguez

FOREIGN

New Zealand Embassy
ATTN: W. Norman

DEPARTMENT OF ENERGY CONTRACTORS

Sandia National Labs
ATTN: Div 1223, B. Finley

DEPARTMENT OF DEFENSE CONTRACTORS

Abbott Associates, Inc
ATTN: P. Abbott

Adaptronics, Inc
ATTN: F. Cook

Aerospace Corp
ATTN: G. Fuller
ATTN: Quon Yin Kwan
ATTN: F. Roder
ATTN: R. Moler

Battelle Memorial Institute
ATTN: J Ott

DEPARTMENT OF DEFENSE CONTRACTORS (Continued)

BDM Corp
ATTN: C. Wold

Behavorial Research Assoc, Inc
ATTN: C. Wallach

Booz-Allen and Hamilton, Inc
ATTN: D. Richards

Mission Research Corp
ATTN: R. Hall
ATTN: L. Ewing

Computing Devices Company
ATTN: J. Chalmers

Cypress International
ATTN: V. Holladay
ATTN: P. Lowry

General Research Corp
ATTN: F. Bick

E-Systems, Inc
ATTN: D. Buehler

Ensco, Inc
ATTN: D. Garges
ATTN: W. Hernandez

Human Factors Research, Inc
ATTN: R. Mackie

Harold Rosenbaum Assoc, Inc
ATTN: T. Midura

DEPARTMENT OF DEFENSE CONTRACTORS (Continued)

JAYCOR
ATTN: L. Blankenship

JAYCOR
ATTN: M. Davis
ATTN: R. McGowan
ATTN: T. Williams

Mission Research Corp
ATTN: P. Benner
ATTN: D. Solomonson

NUSAC, Inc
ATTN: D. Cavileer

New York University
ATTN: R. Murphy

R&D Associates
ATTN: D. Shoemaker

Science Applications, Inc
ATTN: M. Pilgrim

Sylvania Systems Group
ATTN: D. Duff
ATTN: B. Marion
ATTN: R. Miller

TRACOR, Inc
ATTN: J. Albanese